JOÃO LUIZ REBELATTO

CODIFICAÇÃO DE REDE BASEADA EM CÓDIGOS CORRETORES DE ERROS CLÁSSICOS

FLORIANÓPOLIS
2010

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Codificação de Rede Baseada em Códigos Corretores de Erros Clássicos

Tese submetida à
Universidade Federal de Santa Catarina
como parte dos requisitos para a obtenção
do grau de Doutor em Engenharia Elétrica

João Luiz Rebelatto

Florianópolis, 16 de dezembro de 2010.

CODIFICAÇÃO DE REDE BASEADA EM CÓDIGOS CORRETORES DE ERROS CLÁSSICOS

João Luiz Rebelatto

Esta Tese foi julgada adequada para a obtenção do título de Doutor em Engenharia Elétrica, área de concentração Comunicações e Processamento de Sinais, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Santa Catarina.

Bartolomeu Ferreira Uchôa Filho, Ph.D.
Orientador

Roberto de Souza Salgado, Ph.D.
Coordenador do Programa de Pós-Graduação em Engenharia Elétrica

Banca examinadora

Bartolomeu Ferreira Uchôa Filho, Ph.D.
Presidente

Danilo Silva, Ph.D.

Leonardo Silva Resende, D.Sc.

Cecilio José Lins Pimentel, Ph.D.

Richard Demo Souza, D.Sc.

Florianópolis, 16 de dezembro de 2010

Agradecimentos

Gostaria de expressar os meus mais sinceros agradecimentos a todos que, de uma forma ou outra, contribuíram para a realização deste trabalho, em especial

aos meus pais Lírio e Maria Teresinha, e aos meus irmãos Jorge a Ana, pelo imensurável carinho e irrestrito apoio;

a Bartolomeu Ferreira Uchôa Filho, por ter se mostrado muito mais que um excelente orientador: um grande amigo, uma pessoa correta, um exemplo a ser seguido;

a Richard Demo Souza, pelo apoio, amizade e por fazer despertar em mim o interesse pela área acadêmica;

a Andrei Piccinini Legg, Bruno Sens Chang, César Humberto Vidal Vargas, Gustavo Corrêa Lima, Pedro Giassi Junior, Roberto Wanderley da Nóbrega, Wilson Leonel Enriquez Lopez e demais colegas do GPqCom, pela convivência sempre harmoniosa e pelos momentos de confraternização. Em especial a Roberto Wanderley da Nóbrega, pelas valiosas discussões e sugestões que muito contribuíram para o melhoramento do meu trabalho;

aos professores Leonardo Silva Resende e Carlos Aurélio Faria da Rocha, pela agradável convivência e conselhos sempre construtivos;

aos professores Cecílio Pimentel, Danilo Silva, Leonardo Silva Resende e Richard Demo Souza, pelas valiosas sugestões decorrentes da participação na banca examinadora;

aos meus queridos amigos da Lapa e de Curitiba, pelo amizade e companheirismo;

ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pelo apoio material.

Resumo da Tese apresentada à UFSC como parte dos requisitos necessários para obtenção do grau de Doutor em Engenharia Elétrica

CODIFICAÇÃO DE REDE BASEADA EM CÓDIGOS CORRETORES DE ERROS CLÁSSICOS

João Luiz Rebelatto

16 de dezembro de 2010

Orientador: Bartolomeu Ferreira Uchôa Filho, Ph.D.
Área de concentração: Comunicações e Processamento de Sinais
Palavras-chave: codificação de rede, códigos corretores de erros, comunicação cooperativa, diversidade, múltiplo-acesso.
Número de páginas: xxii + 97

Nesta tese, codificação de rede é utilizada para melhorar o desempenho de erro de uma rede em que múltiplos usuários possuem informações independentes para enviar para uma estação-rádio-base (ERB) em comum através de canais sujeitos a desvanecimento em bloco (quase-estático). Considerando que os usuários são aptos a cooperar entre si, o objetivo é aumentar a ordem de diversidade do sistema sem que a taxa de transmissão precise ser reduzida. O esquema proposto nesse trabalho, denominado codificação de rede dinâmica e generalizada (GDNC), é uma generalização dos códigos de rede dinâmicos (DNC) recentemente propostos por Xiao e Skoglund. O projeto dos códigos de rede que maximizam a ordem de diversidade é reconhecido como equivalente ao projeto de códigos de bloco lineares sobre um campo finito não-binário sob a métrica de Hamming. Prova-se que adotar uma matriz geradora sistemática de um código com máxima distância mínima (código MDS) sobre um campo finito suficientemente grande como matriz de transferência da rede é uma condição suficiente para atingir diversidade completa em um modelo em que os enlaces estão sujeitos a falhas. A generalização proposta oferece uma solução de compromisso entre taxa de transmissão e ordem de diversidade, sendo que ambos podem ser selecionados para serem maiores que no esquema DNC. A influência de um canal de retorno entre a ERB e os usuários é também

avaliada, e mostra-se que se a ERB for capaz de transmitir uma pequena quantidade de informação para os usuários, pode-se aumentar a taxa de transmissão ainda mais, sem que a ordem de diversidade seja reduzida. Uma análise da probabilidade de *outage* mostrando o melhor desempenho dos esquemas propostos é efetuada, a qual é suportada por resultados de simulações computacionais.

Abstract of Thesis presented to UFSC as a partial fulfillment
of the requirements for the degree of Doctor in Electrical Engineering

NETWORK CODING BASED ON CLASSICAL ERROR CORRECTING CODES

João Luiz Rebelatto

December 16th, 2010

Advisor: Bartolomeu Ferreira Uchôa Filho, Ph.D.
Area of concentration: Communications and Signal Processing
Keywords: network coding, error correcting codes, cooperative communication, diversity order, multiple access.
Number of pages: xxii + 97

In this dissertation, network coding is applied to a network consisting of multiple users sending different information to a common base station (BS) through independent block fading channels in order to improve its error performance. Considering that the users are able to cooperate, the aim is to increase the diversity order of the system without reducing its code rate. The proposed scheme, called generalized dynamic-network coding (GDNC), is a generalization of the dynamic-network codes (DNC) recently proposed by Xiao and Skoglund. The design of the network codes that maximizes the diversity order is recognized as equivalent to the design of linear block codes over a nonbinary finite field under the Hamming metric. It is proved that adopting a systematic generator matrix of a maximum distance separable block code over a sufficiently large finite field as the network transfer matrix is a sufficient condition for full diversity order under a link failure model. The proposed generalization offers a much better tradeoff between rate and diversity order compared to the DNC. The influence of a feedback channel between the BS and the users is also evaluated, and it is shown that if the BS is able to transmit a small amount of information back to the users, the transmission rate can be increased even further, without reducing the diversity order of the system. An outage probability analysis showing the improved performance is carried out, and computer simulations results are shown to agree with the analytical results.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

AAF	*Amplify-and-forward*
Anatel	Agência Nacional de Telecomunicações
BC	*Broadcast*
BCH	*Bose-Chaudhuri-Hocquenghem*
BNC	*Binary network coding*
BPSK	*Binary phase shift keying*
CRC	*Cyclical redundancy check*
CSI	*Channel state information*
DAF	*Decode-and-forward*
DNC	*Dynamic network code*
ECC	*Error correcting coding*
ERB	Estação-rádio-base
FER	*Frame erasure rate*
GDNC	*Generalized dynamic network coding*
i.i.d.	independente e identicamente distribuído
LDPC	*Low density parity check*
LIF	*Linear information flow*

LLR *Logarithm likelihood ratio*

MAC *Multiple access*

MDS *Maximum distance separable*

MIMO *Multiple-input multiple-output*

RNC *Random network coding*

SIC *Successive interference cancelation*

SNR *Signal-to-noise ratio*

TS *slot* de tempo

Capítulo 1

Introdução

A IMPORTÂNCIA e a influência dos sistemas de comunicação na evolução da humanidade e formação do mundo como o vemos hoje é gigantesca. A evolução de tais sistemas fez com que barreiras fossem quebradas, distâncias encurtadas, fato que sem sombra de dúvida pode ser visto como um dos pilares para o processo de globalização mundial ocorrido nas últimas décadas.

Grande parte da população mundial é dependente de redes de comunicação de dados no seu cotidiano, seja para se deslocar (utilizando o sistema GPS, por exemplo), para controlar suas finanças (*netbank*) ou para garantir a segurança de sua residência (rede de sensores) ou de seus automóveis (rastreamento), dentre outros. E se a parcela da população que depende diretamente de redes de comunicação no seu dia-a-dia já é grande, tende a se tornar ainda maior.

Esse crescimento na demanda das redes de comunicação pode ser ilustrado com base no cenário nacional. De acordo com dados da Agência Nacional de Telecomunicações (Anatel) [1], a porcentagem de domicílios brasileiros com acesso à internet passou de 8,3% em 2001 para 28,3% em 2008, um crescimento de mais de 200% em apenas 7 anos. Já no quesito telefonia, no mesmo período de tempo, a porcentagem de domicílios brasileiros com telefone (fixo ou móvel) passou de 58,9% para 82,1%.

Ainda sobre a telefonia no cenário nacional, de acordo com a Anatel, apesar de a porcentagem de residências com acesso à telefonia (seja ela fixa ou móvel) ter aumentado no período analisado, a porcentagem de residências com telefone fixo caiu de 51,1% em 2001 para 44,4% em 2008.

Por outro lado, o número de domicílios com acesso a telefonia sem fio (móvel) cresceu de 31,1% para 75,5% no mesmo período. Esses dados servem para ilustrar uma tendência no mercado de comunicações: a opção pela mobilidade, por *comunicações sem fio*. Ainda de acordo com dados da Anatel, o ano de 2010 ficará marcado na história da telefonia móvel nacional como o ano em que o número de aparelhos celulares ativos superou o número de habitantes do país.

Além do aumento na quantidade de usuários utilizando tais serviços, os aplicativos atuais exigem taxas (e qualidade) de transmissão cada vez mais elevadas, como ilustrado na Figura 1.1. A evolução se iniciou com o primeiro padrão de telefonia celular (1G) (apenas transmissão de voz, de forma analógica) no início dos anos 80, passou pelo padrão 2G (digital, mas principalmente para transmissão de voz, com velocidade de até 64Kbps), chegou ao padrão 3G (voz e dados e velocidade de até 2Mbps com acesso à internet), e segue rumo à quarta geração (4G) que deve ser apresentada em breve (transmissão multimídia, roaming global e velocidade de até 1Gbps).

Figura 1.1: Aplicativos exigem taxas e qualidade de transmissão cada vez mais elevadas.

Mais que isso, estima-se que a maioria do fluxo de informações que trafega pelas redes de comunicações seja proveniente de comunicação entre máquinas [2], e que esse fluxo também tenda a crescer cada vez mais. Atender a toda essa crescente demanda, em se tratando de transmissão por um canal nada amigável como o canal sem fio (o qual apresenta variação temporal, interferências, susceptibilidade a ataques, etc.) é um desafio e tanto, como ilustrado na Figura 1.2. Portanto, é de se esperar que esforços de pesquisas científicas continuem

sendo despendidos para tornar os sistemas de comunicação cada vez mais eficientes, aptos a acomodar uma demanda em crescimento, de forma segura, confiável, e com uma velocidade de transmissão rápida o suficiente.

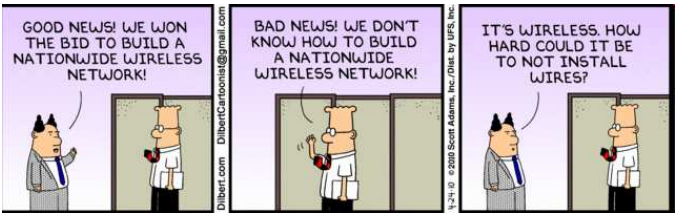


Figura 1.2: O desafio da comunicação por um canal sem fio. Fonte: www.dilbert.com, publicado em 24 de Abril de 2010.

Nesse contexto, a intenção deste trabalho é de levantar alguns pontos importantes da área de comunicações sem fio e propor novas técnicas que contribuam de forma benéfica e possam ser incorporadas às próximas gerações desses sistemas.

1.1 Introdução ao Problema

Mais de 60 anos se passaram desde que, em 1948, Claude Shannon marcou época publicando seu trabalho intitulado *teoria matemática das comunicações* [3], dando origem à Teoria da Informação como a vemos atualmente. Em [3], Shannon introduziu o conceito de **capacidade de canal**, definida como máxima taxa na qual pode-se realizar comunicação de forma confiável, se não houver restrição na complexidade do transmissor e do receptor. Shannon mostrou que para uma taxa R menor que a capacidade de canal, existem códigos de canal com taxa R e com taxas de erro de bloco (ou símbolo) arbitrariamente pequenas.

Desde então, a comunidade científica vem despendendo enormes esforços na busca por códigos corretores de erros que se aproximem da capacidade apresentada por Shannon. Uma quantidade incontável de trabalhos foi publicada (por exemplo, [4–9]) e códigos corretores de erros que praticamente atingem a capacidade de Shannon foram elaborados (tais como códigos turbo [6] e códigos LDPC [4]). Apesar de a área ainda despertar muito interesse por parte da comunidade científica, seja no sentido de obter minúsculas melhoras no desempenho ou uma redução na complexidade de implementação [10–13], a margem para melhoras é realmente muito pequena. Podemos dizer que a capacidade de Shannon

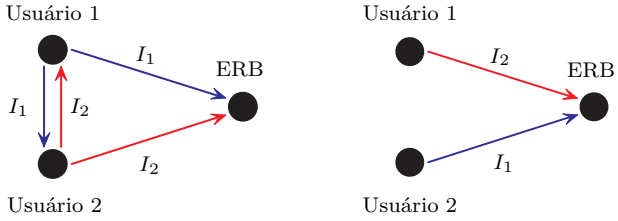
para o canal Gaussiano e comunicação ponto-a-ponto (camada física) foi atingida.

Em uma rede de comunicação com múltiplos usuários, todavia, além da preocupação em garantir a transmissão confiável da informação ponto-a-ponto, cuidados devem ser tomados do ponto de vista da rede como um todo, de forma a torná-la o mais eficiente, o mais segura e o mais rápida possível.

Uma maneira de aumentar a eficiência de redes de comunicação é empregando o conceito de **cooperação**, o qual tem sido largamente aplicado a comunicações sem fio recentemente [14–27], devido à sua robustez ao desvanecimento de canal. Em um sistema de comunicação sem fio cooperativo em que múltiplos usuários possuem informação independente para transmitir para uma estação-rádio-base (ERB) em comum, além de difundir sua própria informação, os usuários ajudam uns aos outros retransmitindo a informação de seus parceiros [14–18]. No protocolo de retransmissão denominado **decodifica-e-encaminha** (DAF, do inglês *decode-and-forward*) [14–16], a palavra-código retransmitida para a ERB é uma versão recodificada da palavra-código recebida (e decodificada) previamente na fase da difusão. Uma rede DAF com 2 usuários está ilustrada na Figura 1.3. No primeiro instante, (Figura 1.3(a)), cada usuário difunde sua própria informação (normalmente por canais ortogonais). No segundo instante de tempo (Figura 1.3(b)), cada usuário transmite a informação de seu parceiro para a ERB após decodificá-la e recodificá-la novamente. Caso certo usuário não seja capaz de decodificar a informação de seu parceiro, ele envia sua própria informação novamente. Como a mesma informação é transmitida por canais independentes, diversidade de cooperação é obtida [14, 15].

Outro enorme passo no sentido de aumentar a eficiência de redes de comunicação foi dado quando, no ano de 2000, Ahlswede, Cai, Li e Yeung [28] apresentaram resultados surpreendentes sobre como uma nova forma de disseminar pacotes de dados por uma rede pode resultar em uma maior vazão de informação. A assim chamada **Codificação de Rede** (do inglês *Network Coding*) logo transcendeu os domínios da teoria de informação, passando a receber contribuições de diversas áreas como codificação, combinatória, criptografia, otimização, ciência da computação e redes, além de aplicações como redes *peer-to-peer*, armazenagem distribuída, redes sem fio, e redes de sensores [29, 30].

Codificação de rede também tem sido aplicada recentemente a sistemas de comunicação sem fio cooperativos para melhorar seus desempenhos em termos de taxa de erro de bit (BER, do inglês



(a) Fase de difusão. (b) Fase de cooperação.

Figura 1.3: Rede cooperativa decodifica-e-encaminha com 2 usuários. (a) Cada usuário difunde sua própria informação e (b) cada usuário transmite a informação de seu parceiro após decodificá-la e recodificá-la.

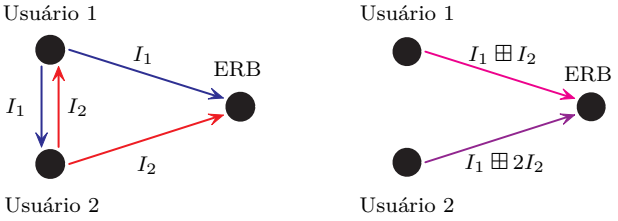
bit error rate) [17–26]. Em um sistema com codificação de rede, os retransmissores são aptos a processar as informações recebidas de diferentes usuários, e transmitir combinações lineares (com coeficientes escolhidos de um campo finito GF(q)) das informações disponíveis.

Um sistema cooperativo com dois usuários que emprega codificação de rede binária (BNC, do inglês *binary network coding*) foi proposto em [17]. Nesse esquema, cada usuário transmite a soma binária (XOR) de sua própria informação e da informação de seu parceiro (caso decodificada corretamente). Ao utilizar BNC, mostra-se que um ganho em termos de BER é obtido se comparado ao esquema DAF, porém, a derivada da curva de BER em função da SNR[1] (SNR, do inglês *signal to noise ratio*) não é aumentada.

Em [19], mostrou-se que codificação de rede binária não é ótima para atingir ordem de diversidade completa em sistemas com múltiplos usuários e múltiplos retransmissores quando falhas nos canais interusuário são levadas em consideração. Um resultado similar foi apresentado em [18], todavia, ao invés de considerar retransmissores dedicados, os próprios usuários atuam como retransmissores uns para os outros. O esquema proposto em [18], denominado **códigos de rede dinâmicos** (DNC, do inglês *dynamic-network codes*), considera um código de rede não-binário e fixo. Um esquema DNC para uma rede com 2 usuários está ilustrado na Figura 1.4.

No primeiro instante de tempo, cada um dos M usuários difunde um único pacote para a ERB, a qual tenta decodificá-lo. Do segundo instante de tempo até o M-ésimo instante, cada usuário, e um de

[1] Ordem de diversidade, definida no Capítulo 4.



(a) Fase de difusão. (b) Fase de cooperação.

Figura 1.4: Rede cooperativa com 2 usuários empregando codificação de rede não-binária. (a) Cada usuário difunde a sua próprio informação e (b) cada usuário transmite uma combinação linear sobre GF(3) composta de todos os pacotes de informação disponíveis.

cada vez, transmite $M-1$ combinações lineares não binárias para a ERB, compostas de todos os pacotes que ele conseguiu decodificar corretamente na fase de difusão e de seu próprio pacote. Com DNC, usando-se um código de rede apropriadamente projetado, foi mostrado que a ordem de diversidade é maior que no caso em que códigos de rede binários são utilizados. O esquema é chamado "dinâmico" no sentido em que o código de rede é projetado para ter um desempenho bom sob a possibilidade de ocorrência de erros nos canais entre os usuários. Todavia, esse procedimento que leva em consideração todos os diferentes padrões de erro nos canais interusuário no projeto do código pode se tornar extremamente complexo à medida em que o número de usuários na rede aumenta.

No exemplo da Figura 1.4, os pacotes transmitidos para a ERB seriam $[I_1 \quad I_2 \quad I_1 \boxplus I_2 \quad I_1 \boxplus 2I_2]$, os quais podem ser representados através do produto $[I_1 \quad I_2]\mathbf{G}_{\text{DNC}}$, em que

$$\mathbf{G}_{\text{DNC}} = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array}\right] \tag{1.1}$$

corresponde à matriz de transferência do sistema.

Do ponto de vista da matriz de transferência do sistema, pode-se fazer uma analogia entre teoria da codificação clássica e códigos de rede [31–34]. A matriz de transferência apresentada em (5.1), por exemplo, pode ser vista como a matriz geradora de um código de bloco linear sobre GF(3) de taxa 2/4 na sua forma sistemática. Em [33, 34], Yeung & Cai derivaram uma generalização dos limitantes de Hamming,

Singleton e Gilbert-Varshamov, estendendo conceitos de teoria de codificação clássica ponto-a-ponto para uma rede de comunicação com múltiplos usuários, e focando na sua capacidade de correção de erro. Em [35], mostrou-se que a distância mínima de um código de correção de erros de rede, para um caso de multidifusão com uma única fonte, exerce a mesma função que na teoria de codificação clássica. O desempenho de decodificação sob a ocorrência de diferente tipos de erros e apagamentos também foi avaliado em [35].

Neste trabalho de doutorado, codificação de rede é utilizada para melhorar o desempenho de erro de uma rede de acesso múltiplo. Em particular, objetiva-se aumentar a ordem de diversidade através de um projeto apropriado das combinações lineares realizadas nos nós da rede. A codificação de rede, que originalmente foi proposta para maximizar o fluxo de informação em uma rede, aqui promoverá um melhor desempenho de erro.

Para tal, uma outra relação entre códigos de rede e códigos corretores de erros clássicos será investigada neste trabalho: a equivalência do problema em questão e do projeto de códigos de bloco lineares sobre GF(q) para correção de apagamentos [36]. Em particular, nota-se que a ordem de diversidade é igual à distância mínima de Hamming do código de bloco para o caso particular em que os canais interusuário são livres de erros. Nessa situação, ferramentas e limitantes da teoria da codificação clássica, tais como o limitante de Singleton [36], podem ser utilizados para avaliar a ordem de diversidade do sistema.

Baseados no limitante de Singleton como um limitante superior para a ordem de diversidade, apresenta-se o esquema GDNC (do inglês *generalized dynamic-network codes*), uma generalização do esquema DNC que é mais flexível em termos de taxa e diversidade, e que, inclusive, pode apresentar tanto taxa quanto ordem de diversidade maiores que as do esquema DNC. Como os canais interusuário não são livres de erros na prática, o limitante de Singleton para a ordem de diversidade não pode ser atingido. Essa diferença entre o limitante e a diversidade atingível pelo esquema GDNC também será quantificada.

Códigos que atingem o limitante de Singleton são chamados de códigos MDS (do inglês *maximum distance separable*) [36]. Com relação ao projeto do código de rede do esquema GDNC, mostra-se que se a matriz geradora de um código MDS (tais como os bem conhecidos códigos Reed-Solomon [37]) é utilizada como matriz de transferência da rede, a máxima ordem de diversidade está garantida. Pelo outro lado, se uma matriz geradora de um código com distância mínima de Hamming menor que a máxima distância mínima for utilizada como matriz de

transferência, a máxima ordem de diversidade não é garantida.

Todavia, em ambos os esquemas DNC e GDNC, uma vez que o código é projetado, ele permanece fixo até que a configuração da rede seja alterada e um novo código seja requisitado. Essa característica apresenta um efeito maléfico sobre a taxa de transmissão média do sistema, uma vez que usuários podem estar transmitindo paridades após a ERB já ter recebido informação suficiente para recuperar todos os pacotes de informação com sucesso. Esses desperdício de recursos aumenta à medida que a SNR aumenta.

Com o intuito de contornar essa limitação, neste trabalho também é proposto um projeto de códigos de rede adaptativos, assumindo a existência de um canal de retorno entre a ERB e os usuários. Através desse canal de retorno, uma pequena quantidade de informação relativa ao sucesso/fracasso na decodificação dos pacotes recebidos pela ERB durante a fase de difusão é transmitida. O objetivo é aumentar a taxa média do código (e consequentemente a taxa do sistema) sem diminuir a ordem de diversidade atingida pelo esquema GDNC original. Nesta extensão do esquema GDNC, o número de pacotes de paridade transmitidos na fase de cooperação é devidamente escolhido de acordo com a informação enviada de volta pela ERB. Expressões analíticas para a taxa média e a ordem de diversidade serão obtidas, as quais serão confrontadas com resultados obtidos através de simulações computacionais.

1.2 Motivação

Trata-se de um tema atual e de grande interesse por parte da comunidade acadêmica e científica. Uma busca pelo tema "*network coding*" no site de procura google, por exemplo, apresenta cerca de 133 mil resultados, um número relevante para um tema relativamente recente. Diversas conferências importantes apresentam sessões exclusivas sobre codificação de rede (ISIT, ITW, Allerton, INFOCOM, Globecom, Mobicom, SIGCOMM, etc) e há também simpósios inteiramente dedicados ao tema (NetCod, WiNC), acomodando mais de 400 artigos por ano desde 2008 [38].

Além disso, esse foi um tema de comum interesse entre o doutorando, seu orientador e o grupo de pesquisa escolhido para realização do doutorado sanduíche (Universidade de Sydney).

Por fim, apesar desse grande interesse por parte da comunidade acadêmica internacional, codificação de rede é um tema que ainda carece de especialistas no Brasil.

1.3 Objetivos

1.3.1 Objetivo Geral

Propor técnicas de codificação de rede utilizando ferramentas de teoria da codificação clássica, com o intuito de melhorar o desempenho dos sistemas de comunicações futuros em comparação aos atuais.

1.3.2 Objetivos Específicos

- Utilizar conceitos de codificação de canal (mais especificamente de códigos de bloco) para esclarecer pontos relativos à codificação de uma rede de múltiplo-acesso;
- Estender o esquema DNC, propondo um esquema capaz de atingir ordem de diversidade e taxa de transmissão mais altas que o esquema original;
- Avaliar o desempenho do esquema proposto analiticamente;
- Confrontar os resultados obtidos analiticamente com simulações computacionais.

1.4 Contribuições

Resultados preliminares sobre a relação entre códigos de rede e códigos corretores de erros clássicos foram publicados recentemente em [20], em que mostrou-se que a ordem de diversidade é igual à distância mínima de Hamming do código de bloco para o caso particular em que os canais interusuário são livres de erros.

Baseados no limitante de Singleton como um limitante para a ordem de diversidade, propôs-se o esquema GDNC em [20], o qual é capaz de atingir tanto ordem de diversidade quanto taxa de transmissão mais elevadas que o esquema DNC [18].

Com relação ao projeto do código de rede do esquema GDNC, foi mostrado em [21] que se a matriz geradora de um código MDS é utilizada como matriz de transferência da rede, a máxima ordem de diversidade está garantida.

Em [23] elaborou-se sobre o esquema GDNC através da suposição de existência de um canal de retorno entre a ERB e os usuários. Utilizando a informação recebida da ERB, cada usuário é capaz de projetar as combinações lineares de forma adaptativa, tal que a taxa média do código seja aumentada o máximo possível e a ordem de diversidade mantida igual à do esquema GDNC original.

No esquema GDNC, assume-se que para cada enlace da rede existe um código de canal capaz de recuperar a informação caso o ganho do canal do enlace correspondente esteja acima de um certo limiar. Em [39], códigos corretores de erros que se aproximam da capacidade de canal

(códigos convolucionais irregulares concatenados em série [9]) foram incorporados ao esquema GDNC, comprovando os resultados obtidos em [20, 21].

Outros trabalhos foram também publicados durante o período de doutorado [22, 40, 41], mas não se relacionam diretamente com o tema da tese.

As contribuições realizadas durante o período de doutorado estão sumarizadas na sequência:

- Artigos completos publicados em anais de conferências: 4 (2 internacionais + 2 nacionais) [20, 22, 40, 41];
- Artigos submetidos para conferências[2]: 2 (internacionais) [23, 39];
- Artigos submetidos para periódicos[2]: 2 (internacionais) [21, 42].

1.5 Estrutura do Documento

Os Capítulos 2 e 3 apresentam uma breve revisão de códigos corretores de erros clássicos (mais especificamente os códigos de bloco lineares, com foco na subclasse de códigos de bloco denominada Reed-Solomon [37]) e de codificação de rede, respectivamente. Devido às restrições de espaço e como o intuito deste trabalho não é reproduzir material já conhecido e publicado, ao leitor interessado em mais detalhes sobre codificação de rede, sugere-se as referências [28–30, 43]. Já para códigos corretores de erros (em particular códigos Reed-Solomon), sugere-se [36, 44].

A descrição de alguns trabalhos e esquemas que serviram como base para a pesquisa desenvolvida nessa tese é apresentada no Capítulo 4. Neste capítulo, o modelo do sistema considerado também é apresentado.

O Capítulo 5 tem como objetivo apresentar o esquema de codificação de rede proposto nesta tese, o qual utiliza conceitos de teoria da codificação clássica no seu projeto. Uma teoria de matriz geradoras com deficiência é desenvolvida a fim de mostrar o desempenho superior do esquema proposto se comparado com os esquemas presentes na literatura. Simulações computacionais também são apresentadas com o intuito de suportar os resultados obtidos de forma analítica.

No Capítulo 6, apresenta-se uma variante do esquema apresentado no Capítulo 5. Aqui, assume-se a existência de um canal de retorno entre a ERB e os usuários, pelo qual é transmitida uma pequena quantidade de informação. Através de uso adequado deste informação proveniente da ERB, mostra-se (analiticamente e através de simulações computacionais) que o desempenho do sistema pode ser melhorado ainda mais.

[2]Aguardando revisão.

Finalmente, o Capítulo 7 apresenta as conclusões e comentários finais desta tese.

Capítulo 2

Códigos de Bloco Lineares

OS códigos corretores de erros (ECC) foram introduzidos por Hamming [45], e se caracterizam pela inserção de redundância na mensagem de informação proveniente da fonte, com o intuito de detectar e/ou corrigir possíveis erros causados durante a sua transmissão por um canal ruidoso. A Figura 2.1 apresenta um sistema de comunicação em sua forma canônica, contendo codificador/decodificador.

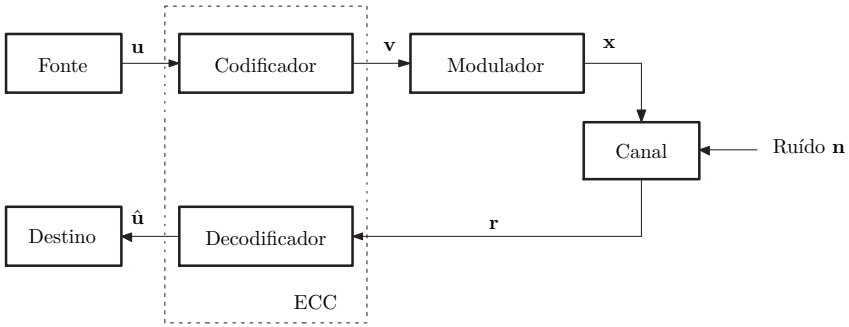


Figura 2.1: Sistema de comunicação digital na forma canônica.

O codificador recebe em sua entrada a sequência de dados vinda da fonte e insere alguma redundância. Dependendo de como a redundância é inserida na mensagem, os códigos corretores de erros podem ser divididos em duas classes [46–49]: os de *bloco* e os *convolucionais*.

Nesta tese, códigos de bloco serão considerados. Como o próprio nome sugere, os códigos de bloco processam a informação bloco-a-bloco,

tratando cada novo bloco de informação independentemente dos outros. Em outras palavras, codificação de bloco é uma operação sem memória, uma vez que as palavras-código são independentes umas das outras.

Na codificação de bloco, a mensagem a ser codificada é agrupada em segmentos de comprimento fixo. Cada mensagem, denotada por $\mathbf{u}$, é composta por k símbolos de informação. O codificador, de acordo com certas regras, transforma a mensagem de entrada $\mathbf{u}$ em uma sequência $\mathbf{v}$, de comprimento n, em que $n \geq k$. A sequência $\mathbf{v}$ é referida como **palavra-código**. Para o conjunto de todas as palavras-código dá-se o nome de **código de bloco**.

No processo de codificação de um código linear, a palavra-código $\mathbf{v}$ é gerada a partir de $\mathbf{u}$ através de certas combinações lineares representadas por

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G} \tag{2.1}$$

em que $\mathbf{G}$ é uma matriz de dimensões $k \times n$ denominada *matriz geradora*.

Um código linear de bloco é dito ser *sistemático* quando parte das palavras-código é formada exatamente pela sequência de informação, como ilustrado na Figura 2.2, em que a sequência de entrada possui comprimento de k símbolos, e a palavra-código comprimento n símbolos, correspondendo a $n - k$ símbolos redundantes[1]. Nesse caso, a matriz

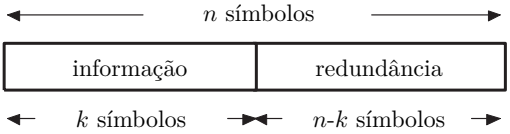


Figura 2.2: Codificador de bloco sistemático.

geradora $\mathbf{G}$ possui a forma

$$\mathbf{G}_{k \times n} = [\mathbf{I}_k | \mathbf{P}_{k \times n-k}] \,, \tag{2.2}$$

em que $\mathbf{I}_k$ corresponde à matriz identidade $k \times k$ e $\mathbf{P}$ à matriz de paridade.

2.1 Distância Mínima de um Código

Um importante parâmetro de um código de bloco é a **distância mínima**, denotada por d_{min}. Este parâmetro determina a capacidade de detecção e correção de erros do código. Seja $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$

[1] Também denominados símbolos de paridade.

uma sequência binária. O **peso de Hamming** (ou simplesmente peso) de $\mathbf{v}$, denotado por $w(\mathbf{v})$, é definido como o número de posições não nulas de $\mathbf{v}$.

Sejam $\mathbf{v}$ e $\mathbf{w}$ duas sequências com comprimento n. A **distância de Hamming** entre $\mathbf{v}$ e $\mathbf{w}$, denotada por $d(\mathbf{v}, \mathbf{w})$, é definida como o número de posições em que as sequências diferem.

Um resultado que será utilizado mais adiante é que a distância de Hamming obedece à desigualdade triangular [44]. Sejam $\mathbf{v}$, $\mathbf{w}$ e $\mathbf{x}$ três sequências de n símbolos. Tem-se que

$$d(\mathbf{v}, \mathbf{w}) + d(\mathbf{w}, \mathbf{x}) \geq d(\mathbf{v}, \mathbf{x}). \tag{2.3}$$

Dado um código de bloco $\mathcal{C}$, pode-se calcular a distância de Hamming entre todas quaisquer duas palavras-código distintas. A distância mínima de $\mathcal{C}$ é definida como

$$d_{min} = \min\{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in \mathcal{C}, \mathbf{v} \neq \mathbf{w}\}. \tag{2.4}$$

Caso o código $\mathcal{C}$ seja linear, a soma de duas palavras-código de $\mathcal{C}$ resulta em uma palavra-código pertencente a $\mathcal{C}$. Assim sendo, a partir de (2.4) temos que [44]

$$\begin{aligned} d_{min} &= \min\{w(\mathbf{v} + \mathbf{w}) : \mathbf{v}, \mathbf{w} \in \mathcal{C}, \mathbf{v} \neq \mathbf{w}\} && \text{(2.5a)} \\ &= \min\{w(\mathbf{x}) : \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq 0\} && \text{(2.5b)} \\ &\triangleq w_{min}, && \text{(2.5c)} \end{aligned}$$

em que $w_{min} \triangleq \min\{w(\mathbf{x}) : \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq 0\}$ é chamado de **peso mínimo** do código $\mathcal{C}$. Em suma, tem-se o seguinte teorema [44]

Teorema 2.1 *A distância mínima de um código de bloco linear é igual ao peso mínimo de suas palavras-código não nulas.*

2.2 Limitante de Singleton

Um importante limitante superior da distância mínima é o limitante de Singleton. Seja $\mathcal{C}$ um código linear com parâmetros (n, k, d_{min}), o limitante de Singleton é dado por [36, Cap.1, Teor.11]:

$$d_{min} \leq n - k + 1. \tag{2.6}$$

Um código que atinge o limitante de Singleton para a distância mínima de Hamming é chamado código MDS (do inglês *maximal distance separable*). Códigos MDS são códigos ótimos no sentido de

que possuem a máxima distância mínima de Hamming possível dados os parâmetros n e k. Um código MDS também pode ter as palavras-código separadas em símbolos de mensagem e símbolos de paridade, isto é, possui uma matriz geradora na forma sistemática [36].

Uma importante família de códigos que pertence à classe de códigos MDS é a família de códigos Reed-Solomon (RS) [37].

2.3 Capacidade de Correção e Detecção de um Código

Quando uma palavra-código $\mathbf{v}$ é transmitida por um canal ruidoso, um padrão de erro de l erros resultará em um vetor recebido $\mathbf{r}$ que difere de $\mathbf{v}$ em exatamente l posições. Se a distância mínima do código $\mathcal{C}$ é d_{min}, quaisquer duas palavras-código distintas pertencentes ao código diferem em pelo menos d_{min} posições. Dessa forma, nenhum padrão de erro de $d_{min} - 1$ ou menos erros pode transformar uma palavra-código em outra palavra-código válida. Assim sendo, diz-se que $\mathcal{C}$ é capaz de detectar todos os padrões de $d_{min} - 1$ erros.

Com relação à capacidade de correção do código $\mathcal{C}$ com distância mínima d_{min}, prova-se que $\mathcal{C}$ é capaz de corrigir todos os padrões de t ou menos erros, em que t é dado por [44]

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor, \tag{2.7}$$

com $\lfloor x \rfloor$ representando o maior inteiro menor que x.

2.3.1 Erros *vs.* Apagamentos

Um apagamento corresponde a um erro cuja localização é conhecida, mas o seu valor não. Com relação à capacidade de correção de apagamentos de um código $\mathcal{C}$ com distância mínima d_{min}, pode-se provar que [44, 50]

- (i) $\mathcal{C}$ é capaz de corrigir até $d_{min} - 1$ apagamentos (sem a ocorrência de erros adicionais);
- (ii) Se existem f apagamentos e t erros, $\mathcal{C}$ é capaz de corrigí-los desde que $2t + f < d_{min}$.

2.4 Operações em Campos Finitos

Operações em campos finitos, também chamados de corpos finitos ou ainda campos de Galois (em homenagem a Évariste Galois), são largamente utilizadas na construção e decodificação de códigos. Em [36], a seguinte definição é apresentada:

Definição 1 *Um campo é um conjunto de elementos no qual é possível somar, subtrair, multiplicar e dividir (exceto a divisão por 0 não é*

definida). Adição e multiplicação devem satisfazer as propriedades comutativa, associativa e distributiva: Para quaisquer α, β, γ *pertencentes ao campo, tem-se que*

$$\begin{gathered}\alpha+\beta=\beta+\alpha, \qquad \alpha\beta=\beta\alpha,\\ \alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma, \qquad \alpha(\beta\gamma)=(\alpha\beta)\gamma,\\ \alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma;\end{gathered}$$

e além disso os elementos 0, 1, $-\alpha$, α^{-1} *(para todo* α*) devem existir tal que*

$$\begin{gathered}0+\alpha=\alpha, \qquad (-\alpha)+\alpha=0, \qquad 0\alpha=0,\\ 1\alpha=\alpha, \qquad (\alpha^{-1})\alpha=1 \text{ (se } \alpha\neq 0).\end{gathered}$$

Um campo finito contém um número finito de elementos, o qual é chamado de ordem do campo.

Em geral, um campo com q elementos é representando por $\mathrm{GF}(q)$ ou $\mathbb{F}_q$.

Mais detalhes sobre campos finitos (ou de Galois) podem ser encontrados no Apêndice A, bem como nas referências [44, 51].

2.5 Códigos Reed-Solomon

Códigos Reed-Solomon podem ser classificados como uma subclasse dos códigos BCH.

2.5.1 Histórico

Os códigos BCH binários foram descobertos por volta de 1960 por Hocquenghem [52] e independentemente por Bose e Ray-Chaudhuri [53, 54], e foram generalizados para todos os campos finitos por Gorenstein e Zierler [55]. Praticamente ao mesmo tempo em que os códigos BCH surgiram na literatura, Reed e Solomon [37] publicaram seu trabalho sobre os códigos que agora carregam os seus nomes. Esses códigos, que podem ser classificados como subclasse dos códigos BCH, na verdade foram previamente construídos por Bush [56] em 1952 no contexto de matrizes ortogonais. Devido à sua capacidade de correção de erros em rajada, códigos Reed-Solomon são utilizados para melhorar a confiabilidade de CDs (do inglês *compact disc*), fitas de audio digitais e outros sistemas de armazenamento de dados [57, 58].

2.5.2 Definição

Códigos BCH (e consequentemente Reed-Solomon) são classificados como **códigos cíclicos**, isto é, possuem a propriedade de que um

deslocamento cíclico de qualquer uma de suas palavras-código resulta em outra palavra-código também pertencente ao código [36]. Essa propriedade simplifica a sua construção, bem como é capaz de reduzir a complexidade de decodificação.

Ao leitor interessado em detalhes sobre códigos BCH, muitas são as referências presentes na literatura, por exemplo, [36, Cap.9] e [58, Cap.5]. Neste trabalho, apenas a subclasse de códigos BCH não-binários definidos sobre GF(q) e de comprimento $n = q - 1$ será considerada. Os códigos pertencentes a essa subclasse são denominados códigos Reed-Solomon, e são os representantes de melhor desempenho dentre os códigos BCH.

De acordo com o citado na Seção 2.2, códigos RS são códigos MDS, ou seja, são códigos com máxima distância mínima de Hamming. Assim sendo, de acordo com (2.7), a capacidade de correção de um código RS é dada por

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{n - k + 1 - 1}{2} \right\rfloor = \left\lfloor \frac{n - k}{2} \right\rfloor . \tag{2.8}$$

Rearranjando os termos de (2.8), obtém-se um comprimento de mensagem $k = n - 2t$. De forma resumida, códigos RS definidos sobre GF(q) possuem os seguintes parâmetros [44]:

Comprimento da palavra-código	$n = q - 1$
Comprimento da mensagem	$k = n - 2t$
Distância mínima de Hamming	$d_{min} = n - k + 1$

2.6 Puncionamento

Seja $\mathcal{C}$ um código (n, k, d_{min}) sobre GF(q). Pode-se puncionar $\mathcal{C}$ apagando-se a mesma coordenada i em todas as palavras-código, resultando em um código $\mathcal{C}^*$ também linear e de comprimento $n - 1$. Seja $\mathbf{G}$ a matriz geradora de $\mathcal{C}$, a matriz geradora de $\mathcal{C}^*$ é obtida através da remoção da coluna i (e omissão de alguma possível linha nula ou duplicada). De forma resumida, o seguinte resultado é apresentado com relação à operação de puncionamento [58]:

Teorema 2.2 *Seja $\mathcal{C}$ um código (n, k, d_{min}) sobre GF(q) e $\mathcal{C}^*$ o código $\mathcal{C}$ puncionado na i-ésima coordenada.*

(*i*) *Se $d_{min} \geq 1$, $\mathcal{C}^*$ é um código $(n - 1, k, d^*_{min})$ em que $d^*_{min} = d_{min} - 1$ caso a i-ésima coordenada da palavra-código de peso mínimo de $\mathcal{C}$ seja não-nula, e $d^*_{min} = d_{min}$ caso contrário.*

(*ii*) *Quando* $d_{min} = 1$, $\mathcal{C}^*$ *é um código* $(n-1, k, 1)$ *caso* $\mathcal{C}$ *não possua nenhuma palavra-código de peso 1 cujo elemento não-nulo é na* i*-ésima coordenada; caso contrário, se* $k > 1$, $\mathcal{C}^*$ *será um código* $(n-1, k-1, d^*_{min})$ *com* $d^*_{min} \geq 1$.

Como exemplo, seja $\mathcal{C}$ um código $(5, 2, 2)$ sobre GF(2) com matriz geradora $\mathbf{G}$ dada por

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \tag{2.9}$$

Sejam $\mathcal{C}^*_1$ e $\mathcal{C}^*_5$ códigos resultantes do puncionamento de $\mathcal{C}$ nas posições 1 e 5, respectivamente. Estes novos códigos possuem matrizes geradoras

$$\mathbf{G}^*_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{e} \quad \mathbf{G}^*_5 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \tag{2.10}$$

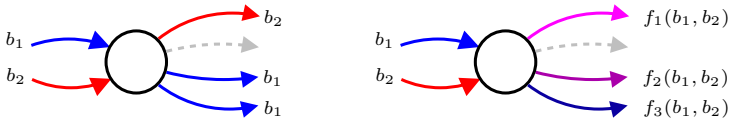
Ou seja, $\mathcal{C}^*_1$ é um código $(4, 2, 1)$ enquanto $\mathcal{C}^*_5$ é um código $(4, 2, 2)$.

Capítulo 3

Codificação de Rede

NAS redes de comunicação atuais, a propagação da informação é tradicionalmente realizada através de um método denominado **roteamento**, em que a informação é armazenada pelos nós intermediários e posteriormente encaminhada para os nós seguintes até que atinja seu destino. Acreditava-se até poucos anos atrás que o processamento da informação nos nós intermediários não trouxesse benefícios na replicação e difusão dos dados [33].

Todavia, em [28], Ahlswede, Cai, Li & Yeung derrubaram esse paradigma demonstrando que tal processamento é necessário para que uma maior vazão nos dados possa ser obtida, dando origem à denominada **codificação de rede** (do inglês *network coding*). Em outras palavras, os dados que são independentemente produzidos e "consumidos" não precisam ser necessariamente mantidos separados enquanto eles são transportados pela rede. Há maneiras de combiná-los e depois extrair as informações originais de forma independente. A Figura 3.1 ilustra a diferença entre um nó roteador e um nó codificador.



(a) Nó roteador. (b) Nó codificador.

Figura 3.1: Nó da rede operando como (a) roteador (b) codificador.

Com codificação de rede, diversos tipos de ganhos podem ser obtidos, seja em termos de vazão, segurança, desempenho de erro, etc [29].

3.1 Teorema *maxflow-mincut*

O Teorema **maxflow-mincut** é um importante resultado do problema do fluxo máximo em uma rede de unidifusão (uma fonte e um destino). De acordo com tal teorema, dados dois nós quaisquer F e R da rede, o valor do máximo fluxo entre F e R coincide com o valor do mínimo corte entre F e R. Caso os canais da rede possuam a mesma capacidade, o Teorema *maxflow-mincut* pode ser reformulado como se segue [29, 59].

Teorema 3.1 *(maxflow-mincut) O número mínimo de canais que, quando removidos, separam o nó fonte F do nó destino R é igual ao número máximo de caminhos disjuntos de F a R.*

Considere o exemplo da Figura 3.2, a qual apresenta uma rede de unidifusão em que o nó fonte F deseja transmitir informação ao nó destino R. Suponha que cada canal da rede (ramo interligando dois nós) seja capaz de transportar até um bit. De acordo com o Teorema *maxflow-mincut*, existem apenas 3 caminhos disjuntos entre F e R (valor do corte mínimo). Assim, a melhor alternativa seria rotear os 3 bits por tais caminhos, como indicado na figura.

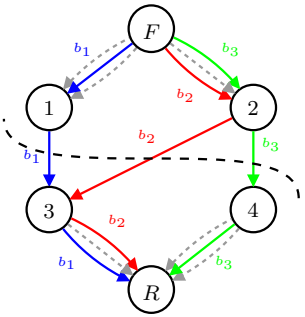


Figura 3.2: Corte mínimo em rede de unidifusão.

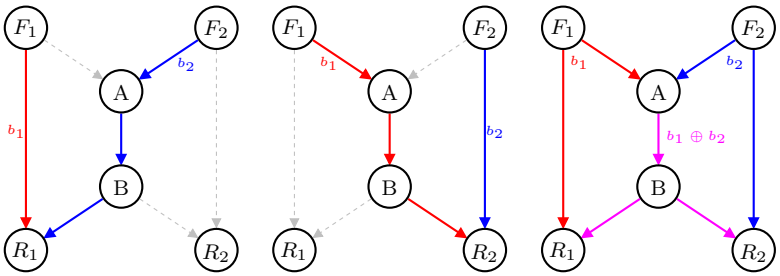
De forma semelhante, pode-se dizer que $\text{maxflow}(F, R) = 3$. Para mais detalhes sobre o Teorema *maxflow-mincut*, sugere-se as referências [29, 60].

3.2 A Rede Borboleta

Para uma rede de unidifusão, como mostrado na seção anterior, roteamento é suficiente para atingir o fluxo máximo da rede. Porém, em redes com múltiplas fontes e/ou múltiplos destinos, codificação de rede pode ser necessária [28].

Os primeiros benefícios de codificação de rede foram demonstrados em termos de vazão em uma rede de multidifusão (uma ou mais mensagens independentes sendo transmitidas por uma única fonte para mais de um destino), através do exemplo da rede borboleta [28]. Tal exemplo está reproduzido na Figura 3.3, a qual representa uma rede de comunicação na forma de um grafo direcionado, no qual os vértices correspondem aos nós da rede (terminais) e as arestas representam os canais. A rede é composta por duas fontes (F_1 e F_2) e dois destinos (R_1 e R_2). Assume-se que as fontes F_1 e F_2 podem enviar somente um bit por instante de tempo, denotados por b_1 e b_2, respectivamente.

Se o receptor R_1 utiliza todos os recursos da rede para si próprio, ele pode receber a informação de ambas as fontes, de acordo com o apresentado na Figura 3.3(a). O mesmo acontece para o receptor R_2 na Figura 3.3(b).



(a) Roteamento para R_1. (b) Roteamento para R_2. (c) Codificação de rede.

Figura 3.3: Rede borboleta. As fontes F_1 e F_2 realizam a difusão de suas mensagens para os receptores R_1 e R_2. Adaptado de [29].

Agora, se ambos os receptores precisam receber os sinais de ambas as fontes (multidifusão), há uma limitação no ramo AB, visto que através deste ramo pode-se enviar somente um bit por instante de tempo e deseja-se enviar simultaneamente o bit b_1 para o receptor R_2 e o bit b_2 para o receptor R_1.

Tradicionalmente, o fluxo de informação era tratado de forma semelhante a redes hidráulicas ou até mesmo tráfego de automóveis [61,

62]. Informações independentes eram mantidas separadas. Aplicando este conceito ao exemplo em questão, somente um dos bits b_1 e b_2 poderia ser enviado pelo ramo AB por instante de tempo.

Em [28], foi observado que os nós intermediários podem ser aptos a processar as informações recebidas, ao invés de simplesmente as encaminharem. No exemplo da Figura 3.3(c), o nó A pode realizar a operação XOR (adição no campo binário, denotada por $\oplus$) com os bits b_1 e b_2 e criar um terceiro bit $b_3 = b_1 \oplus b_2$. O receptor R_1 poderia recuperar b_1 e b_2 ao receber $\{b_1, b_1 \oplus b_2\}$. De forma análoga, o receptor R_2 poderia recuperar b_1 e b_2 a partir de $\{b_2, b_1 \oplus b_2\}$.

O exemplo anterior mostra que ao permitir que nós intermediários combinem informações e as mesmas possam ser extraídas nos receptores, um ganho em termos de taxa de transmissão é obtido. Além do aumento no fluxo de informação, codificação de rede tem sido utilizada atualmente para outros fins, tais como aumentar a segurança e prover um melhor desempenho de erro em redes sem fio. Neste trabalho de doutorado, códigos de rede serão utilizados com o intuito de melhorar o *desempenho de erro* de uma rede sem fio com múltiplos usuários, através de uma analogia com códigos corretores de erros clássicos. Portanto, alguns conceitos e trabalhos importantes nessa linha são apresentados no que se segue.

3.3 Erros em Codificação de Rede

Em [31], Cai & Yeung abordaram de forma conjunta as áreas de codificação de rede e codificação de canal pela primeira vez. No trabalho, expandido em [32–34], mostrou-se a grande relação existente entre a teoria de codificação de rede e teoria de codificação clássica (codificação algébrica). Foi mostrado que, na verdade, codificação algébrica pode ser vista como um caso particular de codificação de rede. Tal associação foi realizada considerando-se uma rede de multidifusão com somente uma fonte transmissora e múltiplos receptores, como mostrado na Figura 3.4. Assumindo-se que existem k canais imaginários no nó fonte F, e que F está conectado a n nós receptores, o efeito de um código linear de bloco clássico (n, k) com matriz geradora $\mathbf{G}$ de dimensões $k \times n$ definida sobre um campo finito $\mathbb{F}_q$ é obtido.

Tradicionalmente, as colunas da matriz geradora $\mathbf{G}$ são indexadas no *tempo*. Na formulação de codificação de rede, entretanto, as mesmas são indexadas no *espaço*. Todavia, é fácil perceber que os símbolos recebidos pelos nós receptores na Figura 3.4 constituem a palavra-código do código de bloco linear clássico. Com o intuito de revelar outras semelhanças entre códigos de rede e códigos corretores de erros, considere a Figura

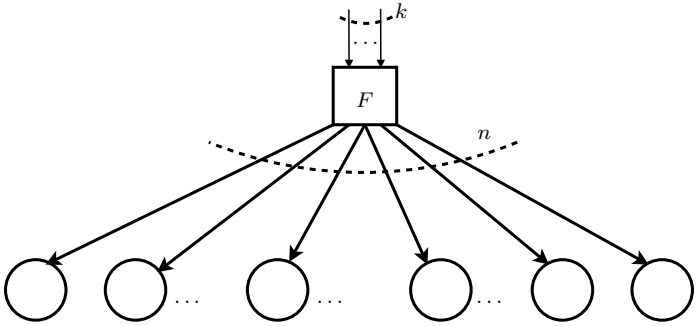


Figura 3.4: Representação em rede de um código linear de bloco clássico. Adaptado de [32].

3.5 (adaptada de [32]), uma extensão da Figura 3.4, em que uma nova camada de $\binom{n}{r}$ nós está presente, cada um destes conectado a r nós (distintos entre si) da camada anterior. Seja um código de bloco linear

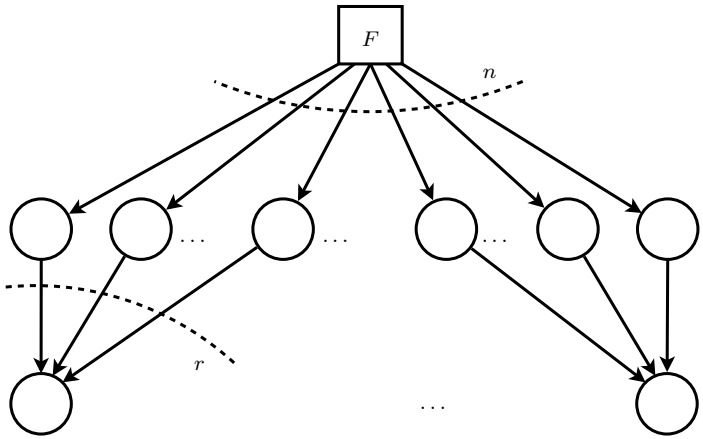


Figura 3.5: Código linear de bloco clássico a partir de uma rede de combinação $\binom{n}{r}$. Adaptado de [32].

(n, k) com distância mínima de Hamming d associado com um código de rede linear de uma rede $\binom{n}{n-d+1}$. Como o código (n, k) possui distância mínima d, acessando um subconjunto de $n - d + 1$ dos nós na camada intermediária (correspondendo a $d - 1$ apagamentos), cada nó receptor R na camada inferior pode decodificar a mensagem $\mathbf{x}$ gerada no nó fonte única e inequivocadamente, em que $\mathbf{x}$ é composto pelos k símbolos de

F. Assim,

$$\text{maxflow}(R) \geq k. \tag{3.1}$$

Como

$$\text{mincut} = n - d + 1, \tag{3.2}$$

obtém-se a partir de (3.1) e (3.2) e do teorema *maxflow-mincut* que

$$d \leq n - k + 1, \tag{3.3}$$

o qual é exatamente o limitante de Singleton para códigos de bloco clássicos, apresentado no Capítulo 2. Assim sendo, o limitante de Singleton pode ser visto como um caso particular do teorema *maxflow-mincut*.

Considere agora a rede da Figura 3.6, a qual corresponde a um sistema de comunicação ponto-a-ponto. Uma mensagem de k símbolos é gerada no nó F e é transmitida para o nó R através de n canais, com a restrição de que $n \geq k$. Se não mais que $(n-k)$ canais forem removidos (de tal forma que $\text{maxflow}(R) \geq k$), a mensagem x pode ser decodificada em R. Equivalentemente, essa rede pode ser descrita como um código de bloco (n, k) que pode corrigir $(n - k)$ apagamentos. Assim sendo, o processo de multidifusão pode ser considerado como uma generalização de um código corretor de apagamentos clássico, mais precisamente, um código MDS (com distância mínima $n - k + 1$).

Figura 3.6: Comunicação ponto-a-ponto (unidifusão). Adaptado de [32].

Assim como códigos corretores de erros clássicos, um código de rede pode ser projetado para correção de *apagamentos* ou para correção de *erros*. Para o primeiro caso, o uso de códigos de detecção de erros aleatórios foi investigado em [43], considerando uma transmissão ponto-a-ponto. Para o segundo caso, generalizações de rede dos limitantes de Hamming, Singleton e Gilbert-Varshamov para códigos corretores de erro clássicos foram obtidos em [32–34]. Propriedades básicas e construção de códigos corretores de erros para redes foram estudadas em [63, 64]. Em [65, 66], um algoritmo para construção de códigos de rede denominado *algoritmo do fluxo de informação linear* (LIF, do inglês *linear information flow*) foi apresentado. Em [30], uma extensão do algoritmo LIF foi considerada para o projeto de códigos de

redes de multidifusão em que os enlaces estão sujeitos a falhas.

Neste trabalho, considera-se uma rede em que múltiplos nós fontes possuem informações independentes para transmitir para um destino em comum (múltiplo acesso). Aqui, os códigos de rede serão projetados para a correção de *apagamentos*. O modelo do sistema será apresentado no próximo capítulo.

Capítulo 4

Preliminares

4.1 Modelo do Sistema

NESTE trabalho considera-se a parte de múltiplo acesso (MAC) de uma rede sem-fio, na qual múltiplos usuários ($M \geq 2$) possuem diferentes informações para transmitir para uma mesma estação rádio-base (ERB), como ilustrado na Figura 4.1.

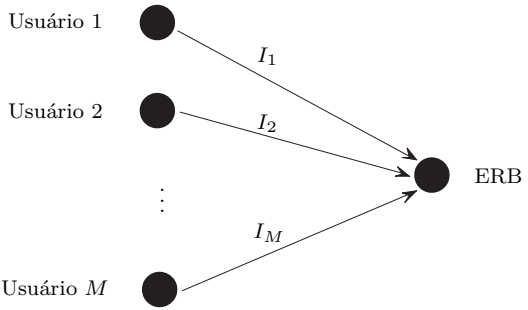


Figura 4.1: Rede de múltiplo acesso, em que múltiplos usuários possuem informações diferentes para transmitir para uma estação rádio-base em comum.

Um *slot* de tempo (TS) é definido como o período de tempo no qual todos os M usuários realizam uma única transmissão, isso é, um TS corresponde a M transmissões. Considera-se também que as transmissões são realizadas por canais ortogonais, seja no

tempo, frequência ou código. Para facilitar o entendimento, considere ortogonalidade temporal. Devido à característica de radiodifusão do meio sem-fio, as mensagens endereçadas à ERB podem ser "ouvidas" pelos demais usuários. A informação "ouvida" pelo usuário i no *slot* de tempo t é dada por

$$y_{j,i,t} = h_{j,i,t}x_{j,t} + n_{j,i,t}, \tag{4.1}$$

em que $j \in \{1, \cdots, M\}$ representa o índice do usuário transmissor e $i \in \{0, 1, \cdots, M\}$ o índice do usuário receptor (0 corresponde à ERB). O índice t denota o *slot* de tempo. $x_{j,t}$ e $y_{j,i,t}$ são os pacotes transmitidos e recebidos, respectivamente. $n_{j,i,t}$ é o ruído Gaussiano aditivo e branco (AWGN) com média zero e variância $N_0/2$ por dimensão. O ganho de canal devido aos multipercursos é denotado por $h_{j,i,t}$, e é assumido possuir distribuição de Rayleigh independente e identicamente distribuída (i.i.d.) (no tempo e no espaço) com variância unitária.

4.1.1 Probabilidade de *Outage*

Assumindo que os $x_{j,t}$'s são variáveis aleatórias Gaussianas i.i.d. e considerando que todos os canais possuem a mesma relação-sinal-ruído (SNR) média, a informação mútua $I_{j,i,t}$ entre $x_{j,t}$ e $y_{j,i,t}$ (máxima taxa com que pode-se transmitir informação de uma forma confiável entre j e i) será [67]

$$I_{j,i,t} = \log(1 + |h_{j,i,t}|^2 \text{SNR}), \tag{4.2}$$

em que a operação log é a abreviação de $\log_2$, o logaritmo na base 2.

Neste trabalho não é considerado o projeto conjunto de códigos de rede e de canal [24–26]. É assumida a existência de códigos de canal poderosos o suficiente para recuperar $x_{j,t}$ sempre que $I_{j,i,t} > R_{j,i,t}$, em que $R_{j,i,t}$ é a taxa de informação do Usuário j para o Usuário i no *slot* de tempo t (taxa com que os bits são codificados no transmissor). Considerando também que todos os usuários possuem a mesma taxa de informação, o índice de R pode ser omitido. Assim, $x_{j,t}$ não será corretamente decodificado pelo usuário i se

$$|h_{j,i,t}|^2 < g, \tag{4.3}$$

em que $g = \frac{2^R - 1}{\text{SNR}}$. A probabilidade desse evento é denominada **probabilidade de** *outage*. Para desvanecimento Rayleigh, a probabilidade de *outage* para o enlace $j \to i$ é calculada como [15, 67]

$$P_e = \Pr\left\{|h_{j,i,t}|^2 < g\right\} = 1 - e^{-g} \approx g, \tag{4.4}$$

em que a aproximação é válida para a região de alta SNR.

4.1.2 Ordem de Diversidade

Considerando-se desvanecimento em bloco, a ordem de diversidade D é definida como [67]

$$D \triangleq \lim_{\mathrm{SNR}\to\infty} \frac{-\log P_o}{\log \mathrm{SNR}}, \tag{4.5}$$

em que $P_o = P_e^{-D}$ é a probabilidade total de *outage* do sistema.

Nesse trabalho, considera-se o caso particular de desvanecimento em bloco no qual os coeficientes de desvanecimento são variáveis aleatórias i.i.d. para diferentes blocos (palavras-código $x_{j,i,t}$ do código de canal empregado nas fontes transmissoras) mas constantes durante o mesmo bloco. Esse caso particular é denominado desvanecimento quase-estático [67, 68]. A menos que seja claramente especificado o contrário, neste trabalho assume-se que os receptores possuem perfeito conhecimento da situação do canal (CSI, do inglês *channel state information*), mas os transmissores não possuem nenhuma CSI.

Antes de continuar, estabelece-se que os operadores $+$ e $-$ representam operações sobre números reais, $\oplus$ é a adição binária (XOR), e $\boxplus$ e $\boxminus$ são as operações de adição e subtração sobre um campo não binário, respectivamente.

As principais considerações apresentadas acima estão resumidas no que se segue.

- (*i*) Considera-se ortogonalidade na transmissão/recepção, de tal forma que cada nó da rede pode apenas transmitir ou receber a informação no mesmo tempo[1], mas não os dois;
- (*ii*) Considera-se que o múltiplo acesso na ERB é ortogonal, ou seja, a mesma recebe mensagens de um usuário por vez (não havendo interferência entre as transmissões);
- (*iii*) O desvanecimento é considerado lento, constante durante um bloco mas i.i.d. no tempo e no espaço para diferentes blocos;
- (*iv*) Transmissores e receptores são equipados com somente uma antena.

Dependência da Taxa de Informação R na Ordem de Diversidade

Seja d o expoente da probabilidade total de *outage*, isto é, $P_o = P_e^d$. De acordo com (4.4), para desvanecimento Rayleigh, tem-se que $P_e \approx$

[1] Ou frequência.

$\frac{2^R-1}{\mathrm{SNR}}$ para a região de alta SNR.

Conforme a definição de ordem de diversidade apresentada em (4.5), tem-se que

$$D \triangleq \lim_{\mathrm{SNR}\to\infty} \frac{-\log P_o}{\log \mathrm{SNR}} \tag{4.6a}$$

$$= \lim_{\mathrm{SNR}\to\infty} \frac{-\log\left(\frac{2^R-1}{\mathrm{SNR}}\right)^d}{\log \mathrm{SNR}} \tag{4.6b}$$

$$= \lim_{\mathrm{SNR}\to\infty} d\left[1 - \frac{\log\left(2^R-1\right)}{\log \mathrm{SNR}}\right] \tag{4.6c}$$

$$= d. \tag{4.6d}$$

Pode-se perceber a partir de (4.6) que a ordem de diversidade D não depende da taxa de informação R nos enlaces entre dois usuários da rede.

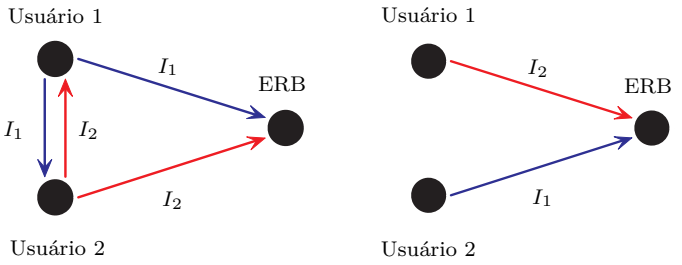
Influência de SNRs Desbalanceadas

Em (4.2), é feita a consideração de que todos os enlaces da rede possuem a mesma SNR média. Tal consideração é certamente irrealista, visto que em um sistema de comunicação sem fio os usuários podem estar a diferentes distâncias da ERB, e podem ou não apresentar linha de visada com a mesma [67]. Porém, através de um procedimento similar ao realizado acima, pode-se mostrar que, independente da SNR dos enlaces, a ordem de diversidade depende apenas do expoente da probabilidade de *outage*.

Na sequência, alguns trabalhos e esquemas que serviram como base para o desenvolvimento deste trabalho serão apresentados. Os mesmos serão úteis para fins de comparação.

4.2 Decodifica-e-Encaminha (DAF)

Uma característica inerente ao canal sem-fio é a da radiodifusão. Essa característica possibilita que determinado usuário, ao enviar uma mensagem para a ERB, tenha essa mensagem "ouvida" pelos outros usuários da rede. Ao ouvir essa mensagem, os outros usuários poderiam retransmiti-la, ao invés de transmitir somente as suas próprias informações. Ao fazer isso, o conceito de cooperação está sendo colocado em prática. Dependendo de qual o procedimento utilizado pelos usuários quando atuando como retransmissores, uma rede cooperativa pode ser classificada de diferentes maneiras. Uma das mais simples está ilustrada na Figura 4.2, para uma rede com 2 usuários. Cada



(a) Fase de difusão. (b) Fase de cooperação.

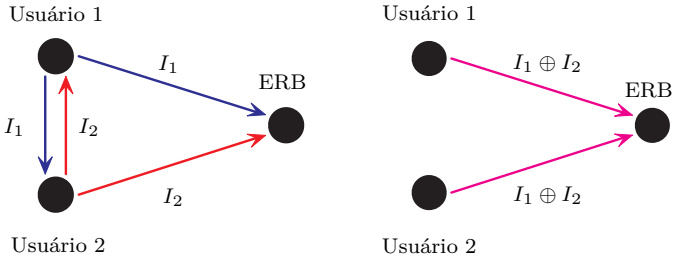
Figura 4.2: Rede cooperativa DAF com 2 usuários. (a) Cada usuário difunde sua própria informação e (b) cada usuário transmite a informação de seu parceiro depois de decodificá-la e recodificá-la.

usuário transmite a sua própria informação no primeiro *slot* de tempo, de acordo com a Figura 4.2(a), por canais ortogonais. Devido à característica de radiodifusão do meio sem-fio, os usuários terão a possibilidade de receber a mensagem de seu parceiro. Caso eles somente amplifiquem e retransmitam essa mensagem sem decodificá-la, tem-se o esquema amplifica-e-encaminha (AAF, do inglês *amplify-and-forward*), o qual não será considerado nesse trabalho. Aqui, considera-se que os usuários tentarão decodificar a mensagem de seus parceiros, e caso a decodificação seja bem sucedida, a informação será recodificada e transmitida no segundo *slot* de tempo, de acordo com a Figura 4.2(b), caracterizando um esquema do tipo decodifica-e-encaminha (DAF, do inglês *decode-and-forward*). Caso um usuário não consiga decodificar corretamente a informação de seu(s) parceiro(s), ele retransmite sua própria informação. O sucesso/falha na decodificação pode ser verificado, por exemplo, através de um verificador de redundância (CRC, do inglês *cyclical redundancy check*). Obviamente, a ERB precisa ser informada sobre qual informação está sendo transmitida.

4.3 Codificação de Rede Binária (BNC)

O esquema apresentado na Figura 4.2 considera apenas *roteamento*. Mensagens independentes são mantidas separadas. Porém, foi mostrado no Capítulo 3 que ao permitir que os usuários processem as diferentes informações, utilizando o conceito de codificação de rede, ganhos podem ser obtidos. Assim sendo, considere a Figura 4.3, a qual apresenta uma rede com 2 usuários em que ambos são aptos a transmitir a soma

binária de sua própria informação e a informação de seu parceiro (se corretamente decodificada) durante o segundo *slot* de tempo.



(a) Fase de difusão. (b) Fase de cooperação.

Figura 4.3: Rede cooperativa com 2 usuários empregando codificação de rede binária. (a) Cada usuário difunde a sua próprio informação e (b) cada usuário transmite uma soma binária (XOR) de sua própria informação e da informação de seu parceiro.

Considerando que os dois canais interusuário são recíprocos, (*i.e.*, $h_{j,i,t} = h_{i,j,t}$), se o canal interusuário não falhar, o que acontece com probabilidade $(1 - P_e)$, os quatro pacotes transmitidos para a ERB são I_1, I_2, $I_1 \oplus I_2$ e $I_1 \oplus I_2$. Considera-se que ao receber duas ou mais cópias da mesma mensagem, a ERB realiza MRC (do inglês *maximum ratio combining*). Nesse caso, uma *outage* para $I_1 \oplus I_2$ ocorre se $|h_{1,0,2}|^2 + |h_{2,0,2}|^2 < g$ e tem probabilidade $P_1 \approx \frac{P_e^2}{2}$ [15, 67].

Sem perda de generalidade, será analisada a probabilidade de *outage* do Usuário 1. O mesmo resultado é válido para o Usuário 2 devido à simetria do problema. Um evento de *outage* ocorre quando a transmissão direta I_1 e pelo menos um dentre I_2 e $I_1 \oplus I_2$ não podem ser recuperados pela ERB. Nesse caso, a probabilidade de *outage* para o Usuário 1 é [18]

$$P_{p,1} \approx P_e(P_e + P_1).$$

Se o canal interusuário está em *outage*, o que ocorre com probabilidade P_e, cada usuário retransmite sua própria informação. Ao receber duas cópias da mesma informação, novamente, a ERB realiza MRC, resultando na seguinte probabilidade de *outage* para o Usuário 1 [15]

$$P_{f,1} \approx \frac{P_e^2}{2}.$$

Considerando todas as possibilidades do canal interusuário, a probabilidade de *outage* para o Usuário 1 é dada por

$$P_{o,1} = (1 - P_e)P_{p,1} + P_e P_{f,1} \approx P_e^2.$$

Caso os canais interusuário não sejam recíprocos, através de uma análise semelhante pode-se mostrar que a probabilidade de *outage* de uma rede com 2 usuários com codificação de rede binária é dada por [17]

$$P_{o,\mathrm{BNC}} \approx P_e^2, \tag{4.7}$$

a qual corresponde a uma diversidade $D = 2$ de acordo com (4.5). Através de uma análise similar, a probabilidade de *outage* do esquema DAF com 2 usuários apresentado na Figura 4.2, considerando canais interusuário não-recíprocos, pode ser mostrada como sendo

$$P_{o,\mathrm{DAF}} \approx 1.5P_e^2, \tag{4.8}$$

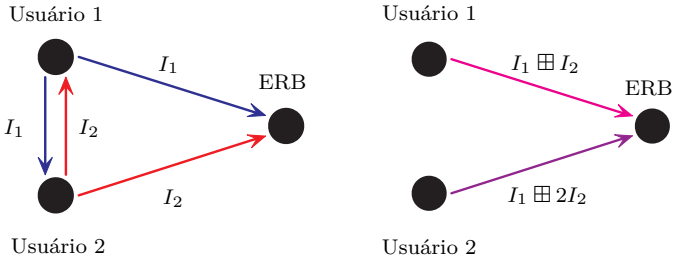
correspondendo também a um valor de diversidade igual a 2.

Pode-se ver que, apesar de codificação de rede em (4.7) apresentar um ganho em termos de taxa de erro se comparada ao esquema DAF (roteamento) em (4.8), a diversidade obtida em ambos os esquemas é a mesma. E mais que isso, não é um valor ótimo, uma vez que a informação de cada usuário é transmitida através de três caminhos independentes e diversidade maior poderia ser atingida, de acordo com o que será apresentado mais tarde.

4.4 Codificação de Rede Dinâmica (DNC)

Em [18], Xiao e Skoglund mostraram que o uso de codificação de rede não-binária é necessário para atingir uma maior diversidade, e então propuseram a chamada Codificação de Rede Dinâmica (DNC, do inglês *dynamic network coding*). A Fig. 4.4 apresenta uma rede com 2 usuários utilizando DNC, em que o tamanho do campo é aumentado e coeficientes não binários são utilizados.

Assumindo canais interusuário perfeitos, a ERB recebe os pacotes I_1, I_2, $I_1 \boxplus I_2$ e $I_1 \boxplus 2I_2$. Pode-se ver que a ERB é capaz de recuperar as mensagens originais I_1 e I_2 a partir de quaisquer 2 dentre os 4 pacotes recebidos. Focando no Usuário 1 (o mesmo resultado vale para o Usuário 2 devido à simetria do sistema), uma *outage* ocorre quando a transmissão direta do pacote I_1 e pelo menos 2 dos 3 pacotes restantes



(a) Fase de difusão. (b) Fase de cooperação.

Figura 4.4: Rede cooperativa com 2 usuários empregando codificação de rede não-binária. (a) Cada usuário difunde a sua próprio informação e (b) cada usuário transmite uma combinação linear sobre GF(3) composta de todos os pacotes de informação disponíveis.

não são decodificados corretamente. Isso ocorre com probabilidade [18]

$$P_0 = P_e \left[\binom{3}{2} P_e^2 (1 - P_e) + P_e^3 \right] \approx 3P_e^3,$$

em que, novamente, a aproximação vale para a região de alta SNR.

Todavia, com probabilidade P_e um usuário não consegue decodificar corretamente o pacote de seu parceiro. Nesta situação, ele retransmite a sua própria informação. A ERB então realiza MRC, resultando na probabilidade de *outage* $P_1 = P_e^2/2$ [15]. Assim sendo, a probabilidade de outage total para o Usuário 1 é [18]

$$P_{o,1} = P_e P_1 + (1 - P_e) P_0 \approx 3.5 P_e^3.$$

É fácil perceber que a diversidade é $D = 3$. Se os canais interusuário não são recíprocos, (*i.e.*, $h_{j,i,t} \neq h_{i,j,t}$), mostra-se no Apêndice B que a probabilidade de *outage* para o esquema DNC com 2 usuários é dada por [18]

$$P_{o,1} \approx 4P_e^3.$$

4.4.1 DNC para Múltiplos Usuários

Expandindo o esquema DNC para uma rede com M usuários, como apresentado em [18], cada usuário transmite $M-1$ combinações lineares na fase de cooperação, de acordo com o ilustrado na Figura 4.5.

Assim sendo, em um sistema DNC com M usuários, a taxa do

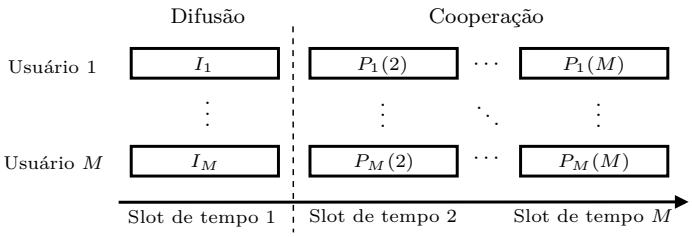


Figura 4.5: Esquema DNC para uma rede com M usuários e taxa $1/M$. $P_i(t)$ corresponde ao pacote transmitido pelo usuário i durante o *slot* de tempo t.

sistema é dada por

$$R_{\text{DNC}} = \frac{\text{nº pacotes de informação}}{\text{nº total de pacotes}} = \frac{M}{M^2} = \frac{1}{M}. \tag{4.9}$$

Com relação à ordem de diversidade, mostrou-se em [18] que para o esquema DNC com taxa $1/M$, a probabilidade de *outage* (e consequentemente a ordem de diversidade) é dominada pela situação em que todos os canais interusuário se encontram em *outage*. Nessa situação, que ocorre com probabilidade P_e^{M-1} (uma vez que são $M-1$ canais interusuário), cada mensagem de informação transmitida para a ERB estaria contida apenas nas M mensagens enviadas pelo próprio usuário que a originou, já que nenhum dos seus parceiros conseguiu decodificá-la corretamente. Dessa forma, foi mostrado em [18] que a ordem de diversidade atingida pelo esquema DNC é

$$D_{\text{DNC}} = 2M - 1, \tag{4.10}$$

porém, com a taxa baixa e fixa dada em (4.9).

O código de rede necessário para atingir a diversidade apresentada em (4.10) foi provado existir através de uma associação entre o esquema DNC e os códigos de rede lineares com fonte única apresentados em [43, Th.11]. O projeto do código de rede proposto em [18] resume-se a encontrar a matriz de transferência que é não-singular para todos os possíveis padrões de erros nos canais interusuário. Esta busca pode ter alta complexidade na medida em que M cresce.

Em [69], Xiao propôs um esquema simplificado para construção de DNC, o qual leva em consideração somente um padrão de *outage* no projeto do código de rede. Tal redução na complexidade de projeto de código é obtida às custas de uma pequena piora no desempenho,

a qual é amenizada à medida que o campo finito que compõe o código torna-se maior, sendo desprezível para um campo suficientemente grande como [69]

$$q \geq \binom{M^2 - 1}{M - 1}. \tag{4.11}$$

Essa abordagem segue na linha dos códigos de rede aleatórios (RNC, do inglês *random network coding*) [28], em que a complexidade de projeto do código de rede é reduzida às custas de um aumento no tamanho do campo finito, aumentando a complexidade das operações tais como decodificação.

No próximo capítulo, um esquema capaz de atingir tanto ordem de diversidade quanto taxa de transmissão mais elevadas que o esquema DNC será proposto, apresentando menor complexidade no projeto do código de rede (utiliza códigos já conhecidos na literatura), bem como reduzindo o tamanho do campo finito necessário para que a ordem de diversidade proposta seja atingida.

Capítulo 5

Codificação de Rede Dinâmica Generalizada (GDNC)

UMA maneira de representar as operações/conexões de uma rede é através de sua matriz de transferência. A matriz de transferência do sistema DNC com 2 usuários apresentado na Figura 4.4, por exemplo, seria dada por

$$\mathbf{G}_{\mathrm{DNC}} = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array}\right]. \tag{5.1}$$

Do ponto de vista de teoria da codificação, pode-se interpretar (5.1) como sendo uma matriz geradora de um código linear de bloco na sua forma sistemática.

No esquema DNC, a ordem de diversidade está relacionada ao número mínimo de pacotes (ou símbolos) recebidos corretamente na ERB a partir dos quais os pacotes de informação de todos os usuários podem ser recuperados. Um pacote que não é recebido corretamente pode ser interpretado como um apagamento, e é descartado pelo receptor. A habilidade do receptor em recuperar os pacotes de informação a partir dos pacotes não apagados é então equivalente à capacidade de correção de apagamento do código de bloco associado. De acordo com o apresentado na Seção 2.3, a palavra-código de um código de bloco linear com distância mínima de Hamming d_{min} pode ser recuperada se no máximo $d_{min} - 1$ de suas posições forem apagadas pelo canal. A conexão entre esses dois problemas estabelece que a ordem de diversidade do sistema DNC com 2 usuários mostrada na Figura 4.4, sob

a suposição de canais interusuário perfeitos, é igual à distância mínima de Hamming do código de bloco de taxa 2/4 com matriz geradora dada em (5.1).

Em geral, para um código de bloco linear de taxa k/n, a distância mínima de Hamming é limitada superiormente pelo limitante de Singleton [44]:

$$d_{min} \leq n - k + 1. \tag{5.2}$$

Como mostrado em [36, Cap.11, Corol.7], o limitante de Singleton somente pode ser atingido se o alfabeto (campo) for grande o suficiente. Por exemplo, para um código de bloco de taxa 4/8, o limitante de Singleton prega que $d_{min} \leq 5$. Todavia, a máxima distância mínima de Hamming possível de ser atingida em GF(2) é 3. Em GF(4), é possível atingir $d_{min} = 4$. O limitante superior $d_{min} = 5$ somente é possível de ser atingido se o tamanho do campo for pelo menos 8 [70].

No esquema DNC, a taxa total é M/M^2. A partir de (5.2), a ordem de diversidade é então limitada superiormente por $D_{\max,\mathrm{DNC}} = M^2 - M + 1$. Observa-se que um sistema com taxa $\alpha M/\alpha M^2$ (para $\alpha \geq 2$) teria a mesma taxa total que o esquema DNC ($1/M$), mas aumentaria o limitante superior da ordem de diversidade para

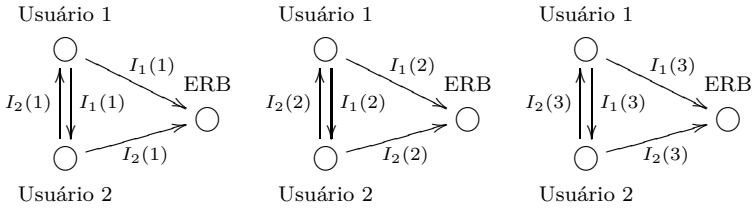
$$D_{\max,\alpha} = \alpha(M^2 - M) + 1. \tag{5.3}$$

Dessa forma, baseando-se no limitante de Singleton como um limitante para a ordem de diversidade, uma generalização do esquema DNC será proposta, a qual se mostrará ser mais flexível em termos de taxa e ordem de diversidade.

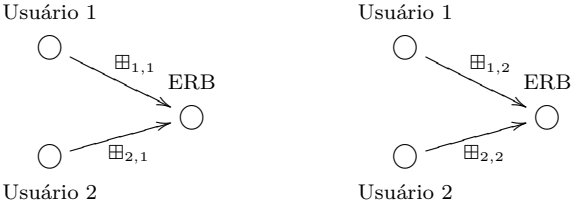
5.1 Introdução à GDNC

Elaborando-se sobre o esquema DNC com 2 usuários apresentado na Figura 4.4, a Figura 5.1 apresenta um exemplo introdutório do esquema proposto nesse trabalho, denominado Codificação de Rede Dinâmica Generalizada (GDNC, do inglês *generalized dynamic-network coding*), uma generalização do esquema DNC. Neste exemplo, cada usuário difunde três pacotes independentes contendo sua própria informação durante a fase de difusão, e depois transmite dois pacotes compostos por combinações lineares (dos seis pacotes difundidos anteriormente, se corretamente recuperados) sobre um campo finito GF($q = 2^b$) na fase de cooperação, em que b é um inteiro maior que zero. O receptor receberá 10 pacotes, os quais podem ser vistos como uma palavra-código de um código de bloco linear sistemático de taxa 6/10.

Sem perda de generalidade, analisa-se a probabilidade de *outage* do



(a) Fase de difusão 1. (b) Fase de difusão 2. (c) Fase de difusão 3.



(d) Fase de cooperação 1. (e) Fase de cooperação 2.

Figura 5.1: Esquema GDNC com taxa 6/10 e $M = 2$ usuários. O símbolo $\boxplus_{m,t'}$ representa a combinação linear de todos os pacotes de informação disponíveis realizada pelo usuário m no *slot* de tempo t', durante a fase de cooperação.

Usuário 1 no primeiro TS. O mesmo resultado é válido para o Usuário 2 devido à simetria do problema em questão. Assume-se inicialmente que os canais interusuário são recíprocos. Nesse caso, a probabilidade de o canal interusuário ser livre de erros é igual a $1 - P_e$. Caso o Usuário 2 consiga decodificar corretamente $I_1(1)$, a mensagem do Usuário 1 no *slot* de tempo 1, então $I_1(1)$ estará em *outage* na ERB se o pacote correspondente à transmissão direta e, no pior caso, os 4 pacotes de paridade contendo $I_1(1)$ não puderem ser decodificados corretamente pela ERB[1], o que ocorre com probabilidade $P_{p,1} \approx P_e^5$.

Se o Usuário 2 não conseguir decodificar corretamente $I_1(1)$, o que acontece com probabilidade P_e, ele não estará apto para ajudar o Usuário 1 retransmitindo $I_1(1)$. Nessa caso, a ERB receberá somente 3 pacotes contendo $I_1(1)$ (a transmissão direta mais 2 pacotes de paridade transmitidos pelo próprio Usuário 1). A mensagem $I_1(1)$ estará em *outage* na ERB se a transmissão direta e, no pior caso, ambos os

[1]Caso o Usuário 2 consiga decodificar corretamente $I_1(1)$, existem outras situações que resultam na mesma probabilidade de *outage* para a mensagem $I_1(1)$. Porém, no momento, a multiplicidade dos padrões de *outage* será deixada de lado e o foco será inteiramente na ordem de diversidade.

pacotes de paridade transmitidos pelo Usuário 1 não forem decodificados também. Esse evento ocorre com probabilidade $P_{f,1} \approx P_e^3$. Assim sendo, considerando canais interusuário recíprocos e todos os padrões de *outage*, a probabilidade de *outage* da mensagem $I_1(1)$ seria dada por

$$P_{o,1} = P_e P_{f,1} + (1 - P_e) P_{p,1} \approx P_e^4. \tag{5.4}$$

Para esse exemplo inicial, quando os canais interusuário não são recíprocos, o mesmo resultado é obtido, de acordo com o apresentado no Apêndice B.

Pode-se ver a partir de (5.4) que a ordem de diversidade obtida pelo esquema GDNC de taxa 6/10 com $M = 2$ usuários apresentado na Figura 5.1 é $D = 4$, a qual é maior que a obtida pelo esquema DNC de taxa 2/4 e $M = 2$ usuários em (4.9). Assim, tanto a taxa quanto a ordem de diversidade foram aumentadas.

5.1.1 Múltiplos Usuários

A generalização do esquema apresentado na Figura 5.1 para o caso em que há $M > 2$ usuários está ilustrada na Figura 5.2. $I_j(t)$ representa a informação (símbolo ou pacote) transmitida pelo Usuário j ($j = 1, \cdots, M$) no *slot* de tempo t ($t = 1, \cdots, k_1$) da fase de difusão (à esquerda), e $P_j(t')$ corresponde à paridade transmitida (símbolo ou pacote) pelo Usuário j no *slot* de tempo t' ($t' = 1, \cdots, k_2$) da fase de cooperação (à direita).

$$\begin{array}{lccc|ccc} \text{User 1:} & I_1(1) & \cdots & I_1(k_1) & P_1(1) & \cdots & P_1(k_2) \\ \text{User 2:} & I_2(1) & \cdots & I_2(k_1) & P_2(1) & \cdots & P_2(k_2) \\ & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \text{User } M\text{:} & I_M(1) & \cdots & I_M(k_1) & P_M(1) & \cdots & P_M(k_2) \end{array}$$
$$\xrightarrow[\text{tempo}]{\textit{slots}\ \text{de}}$$

Figura 5.2: Esquema GDNC para uma rede com M usuários.

Observando a Figura 5.2, cada usuário inicialmente transmite seus próprios k_1 pacotes de informação independentes[2]. Devido à natureza do meio sem fio, os outros usuários terão a possibilidade de "ouvir" estas mensagens e decodificá-las. Na fase de cooperação, cada usuário

[2]Esses pacotes podem ser enviados em qualquer ordem, devido à suposição de canais descorrelacionados tanto no tempo quanto no espaço.

transmite k_2 pacotes de paridade compostos por combinações lineares sobre um campo finito não binário de seus próprios k_1 pacotes e os $k_1(M-1)$ pacotes de informação de seus parceiros (se corretamente decodificados). Caso um usuário não consiga decodificar corretamente um pacote de informação de algum de seus parceiros, este pacote de informação é substituído por um pacote composto somente por zeros na formação da combinação linear. Aqui, assume-se que, assim como em [18], a ERB sabe como cada pacote de informação é formado. Isso pode resultar em algum cabeçalho extra durante a transmissão, porém, se $I_j(t)$ for longo o suficiente, esse cabeçalho extra é desprezível. Assim sendo, a taxa total do esquema GDNC é dada por

$$R_{\text{GDNC}} = \frac{\text{nº pacotes de informação}}{\text{nº total de pacotes}} = \frac{k_1 M}{k_1 M + k_2 M} = \frac{k_1}{k_1 + k_2}. \quad (5.5)$$

A partir de (5.2) e (5.5), pode-se ver que a ordem de diversidade do esquema GDNC é limitada superiormente por

$$D_{\text{GDNC}} \leq k_2 M + 1. \quad (5.6)$$

Entretanto, devido aos possíveis erros nos canais interusuário, esse limitante superior não pode ser atingido. No que se segue, um estudo da probabilidade de *outage* do esquema GDNC será realizado com o intuito de descobrir qual a ordem de diversidade atingida pelo mesmo para uma rede com M usuários.

5.2 Análise da Probabilidade de *Outage*

Seja $D_{j,t} \subseteq \{1, \ldots, M\}$ o conjunto dos índices correspondentes aos usuários que decodificaram $I_j(t)$ com sucesso, o pacote de informação do Usuário j no instante de tempo t durante a fase de difusão. Por conveniência, o índice j também está incluído em $D_{j,t}$. O número de usuários em $D_{j,t}$ é denotado por $|D_{j,t}|$. Seja P_e novamente a probabilidade de *outage* de um único enlace, e denote por $\overline{D}_{j,t}$ o conjunto complementar $\{1, \ldots, M\} \backslash D_{j,t}$, *i.e.*, $\overline{D}_{j,t}$ contém os índices dos usuários que não decodificaram $I_j(t)$ corretamente. A probabilidade de $\overline{D}_{j,t}$ é aproximadamente $P_e^{|\overline{D}_{j,t}|}$. Um novo conjunto $\mathcal{D}_{j,t}(I)$ é definido como sendo o conjunto de todos os pacotes decodificados pelos usuários em $D_{j,t}$ durante a fase de difusão, incluindo $I_j(t)$.

Exemplo 5.1 *Considere uma rede com $M = 5$ usuários, em que $I_1(1)$ (pacote de informação difundido pelo usuário 1 no instante de tempo $t = 1$) foi decodificado corretamente somente pelos usuários de índices 2*

e 4. *Assim, teríamos que* $D_{1,1} = \{1, 2, 4\}$ *e* $\overline{D}_{1,1} = \{3, 5\}$, *de tal forma que* $\Pr\{\overline{D}_{1,1}\} \approx P_e^2$. *Nesta situação, o conjunto* $\mathcal{D}_{1,1}(I)$ *seria composto por todos os pacotes de informação decodificados pelos usuários* 1, 2 *e* 4 *durante a fase de difusão, incluindo o próprio pacote* $I_1(1)$.

Percebe-se que existem pelo menos $|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2$ pacotes contendo mensagens em $\mathcal{D}_{j,t}(I)$ (as próprias $|\mathcal{D}_{j,t}(I)|$ mensagens da parte sistemática mais $|D_{j,t}|k_2$ paridades). Aqui, assume-se que um código de rede bem projetado esteja sendo usado, de tal forma que as $|\mathcal{D}_{j,t}(I)|$ mensagens possam ser recuperadas a partir de quaisquer $|\mathcal{D}_{j,t}(I)|$ pacotes recebidos[3]. Fixando o conjunto $D_{j,t}$ (o que também fixa $\overline{D}_{j,t}$), uma *outage* para $I_j(t)$ é declarada somente quando a transmissão direta $I_j(t)$ e pelo menos $|D_{j,t}|k_2$ dentre os $|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2 - 1$ pacotes recebidos restantes estiverem em *outage*, o que ocorre com probabilidade

$$P_{o,j}(\overline{D}_{j,t}) = P_e\Bigg[\overbrace{\binom{|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2 - 1}{|D_{j,t}|k_2} P_e^{|D_{j,t}|k_2}(1-P_e)^{|\mathcal{D}_{j,t}(I)|-1}}^{|D_{j,t}|k_2 \text{ em } outage} + \dots$$
$$\dots + \underbrace{\binom{|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2 - 1}{|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2 - 1} P_e^{|\mathcal{D}_{j,t}(I)|+|D_{j,t}|k_2-1}(1-P_e)^0}_{\text{Todos os } |\mathcal{D}_{j,t}(I)|+|D_{j,t}|k_2-1 \text{ em } outage}\Bigg] \tag{5.7a}$$

$$\approx P_e\left[\binom{|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2 - 1}{|D_{j,t}|k_2} P_e^{|D_{j,t}|k_2}\right] \tag{5.7b}$$

$$= \gamma(k_1, k_2, \overline{D}_{j,t}) P_e^{(M-|\overline{D}_{j,t}|)k_2+1}, \tag{5.7c}$$

em que $\binom{n}{k}$ é o coeficiente binomial e

$$\gamma(k_1, k_2, \overline{D}_{j,t}) = \binom{|\mathcal{D}_{j,t}(I)| + |D_{j,t}|k_2 - 1}{|D_{j,t}|k_2}$$

é um inteiro positivo que representa o número (multiplicidade) dos padrões de *outage* que resultam na mesma probabilidade. Pode-se ver que $\gamma(k_1, k_2, \overline{D}_{j,t})$ aumenta à medida que $|\mathcal{D}_{j,t}(I)|$ aumenta. Em

[3]No momento, apenas assume-se a existência de tais códigos. A prova de sua existência será mostrada mais adiante.

particular, como $k_1 \leq |\mathcal{D}_{j,t}(I)| \leq Mk_1$, tem-se que

$$\binom{k_1+k_2-1}{k_2} \leq \gamma(k_1,k_2,\{1,\ldots,M\}\backslash\{j\}) \leq \binom{Mk_1+k_2-1}{k_2}. \quad (5.8)$$

Deve-se notar que (5.7) é o pior caso, pois as mensagens $\mathcal{D}_{j,t}(I)$ (exceto $I_j(t)$) podem também ser decodificadas pelos usuários pertencentes a $\overline{D}_{j,t}$, reduzindo a probabilidade de *outage* das mensagens em $|\mathcal{D}_{j,t}(I)|$.

A probabilidade de *outage* é então dada por

$$\begin{aligned} P_{o,j} &= \sum_{\overline{D}_{j,t}} P_e^{|\overline{D}_{j,t}|}(1-P_e)^{(M-1)-|\overline{D}_{j,t}|} P_{o,j}(\overline{D}_{j,t}) && (5.9a)\\ &\approx \sum_{\overline{D}_{j,t}} P_e^{(M-|\overline{D}_{j,t}|)k_2+|\overline{D}_{j,t}|+1}\gamma(k_1,k_2,\overline{D}_{j,t}) && (5.9b)\\ &\approx \gamma'(k_1,k_2,|\overline{D}_{j,t}|^*)P_e^{(M-|\overline{D}_{j,t}|^*)k_2+|\overline{D}_{j,t}|^*+1} && (5.9c)\\ &= \gamma'(k_1,k_2,M-1)P_e^{M+k_2}, && (5.9d) \end{aligned}$$

em que $P_e^{|\overline{D}_{j,t}|}(1-P_e)^{(M-1)-|\overline{D}_{j,t}|}$ é a probabilidade de $|\overline{D}_{j,t}|$ dentre $M-1$ canais interusuário no instante de tempo t estarem em *outage*, e $|\overline{D}_{j,t}|^*$ corresponde ao valor de $|\overline{D}_{j,t}|$ que resulta no termo de menor expoente em (5.9b), o qual, para $k_2 \geq 2$, é $|\overline{D}_{j,t}|^* = M-1$. Para $k_2 = 1$, o expoente em (5.9b) é igual a $M+k_2$ independentemente de $|\overline{D}_{j,t}|$. Finalmente, $\gamma'(k_1,k_2,|\overline{D}_{j,t}|^*)$ coleta as multiplicidades de todos os eventos $\overline{D}_{j,t}$ para os quais $|\overline{D}_{j,t}| = |\overline{D}_{j,t}|^*$. Dessa forma, o seguinte resultado foi provado.

Teorema 5.1 *A diversidade do esquema GDNC para um código de rede apropriadamente projetado e com tamanho de campo suficientemente grande é* $D_{GDNC} = M + k_2$.

Pode-se ver que quando $k_1 = 1$ e $k_2 = M-1$, o esquema proposto se reduz ao esquema DNC, com taxa $k_1/(k_1+k_2) = 1/M$ e ordem de diversidade $M + k_2 = 2M-1$. Em particular, para $k_1 = k_2 = 1$ tem-se o esquema DNC com 2 usuários mostrado na Figura 4.4. A forma com que o esquema GDNC é projetado possibilita a escolha de diferentes valores de k_1 e k_2, resultando em diferentes taxas e diferentes ordens de diversidade. Através de variação independente de k_1 e k_2, pode-se realizar uma troca (*tradeoff*) entre taxa e diversidade. A partir de (5.5) e do Teorema 5.1, pode-se ver que uma escolha apropriada de k_1 e k_2

pode simultaneamente melhorar a taxa e a ordem de diversidade com relação ao esquema DNC.

5.3 Sobre o Projeto do Código de Rede

O Teorema 5.1 mostrou que o esquema GDNC proposto pode atingir diversidade $M + k_2$ desde que o código de rede seja apropriadamente projetado. Nessa seção, o projeto de tais códigos será abordado utilizando ferramentas da teoria clássica de codificação. Inicialmente, algumas propriedades úteis de códigos de bloco lineares serão apresentadas.

Seja $\mathcal{C}$ um código de bloco linear (n, k, d_{min}) sobre GF(q) com matriz geradora sistemática $\mathbf{G}$ dada por:

$$\begin{aligned}\mathbf{G} &= \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & p_{1,1} & p_{1,2} & \cdots & p_{1,n-k} \\ 0 & 1 & \cdots & 0 & p_{2,1} & p_{2,2} & \cdots & p_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{k,1} & p_{k,2} & \cdots & p_{k,n-k} \end{array}\right] \\ &= \left[\begin{array}{c|c} \mathbf{I}_k & \mathbf{P}_{k\times n-k} \end{array}\right]. \end{aligned} \tag{5.10}$$

De acordo com (5.2), a distância mínima de Hamming de $\mathcal{C}$ é limitada superiormente por $d_{min} \leq n - k + 1$. Os códigos que atingem esse limitante são denominados códigos MDS (do inglês *maximum distance separable*). De agora em diante, assume-se que o código $\mathcal{C}$ é MDS. Os seguintes resultados referentes a matrizes geradoras sistemáticas de códigos MDS serão utilizados na sequência do trabalho.

Teorema 5.2 ([36, Cap.11, Teor.8]) *Um código $\mathcal{C}$ (n, k, d_{min}) com matriz geradora $\boldsymbol{G} = [\boldsymbol{I}|\boldsymbol{P}]$, onde $\boldsymbol{P}$ é uma matriz $k \times (n - k)$, é* MDS *se e somente se cada submatriz quadrada de $\boldsymbol{P}$ for não-singular.*

O seguinte lema é uma consequência direta do Teorema 5.2.

Lema 5.1 *Para qualquer código $\mathcal{C}$ (n, k, d_{min}) MDS com matriz geradora $\boldsymbol{G} = [\boldsymbol{I}|\boldsymbol{P}]$, a matriz $\boldsymbol{P}$ não possui nenhum elemento nulo.*

Prova: De acordo com o Teorema 5.2, qualquer submatriz um-por-um de $\mathbf{P}$ é não-singular para códigos MDS. Alternativamente, qualquer linha de $\mathbf{G}$ é uma palavra-código, e deve ter peso de Hamming pelo menos $n - k + 1$. □

5.3.1 Teoria de Matrizes Geradoras Deficientes

Nesta seção, algumas propriedades de novos códigos de bloco obtidos a partir de códigos MDS através da substituição por zeros de alguns

elementos de sua matriz geradora serão apresentadas. Em particular, o objetivo desta seção é obter a distância mínima de Hamming ou a menor capacidade de correção de apagamentos de códigos MDS que podem ser asseguradas quando estes códigos são codificados por um codificador deficiente (com elementos de sua matriz geradora substituídos por zeros). A teoria de matrizes geradoras deficientes que será desenvolvida na sequência servirá como base para o projeto de códigos de rede capazes de maximizar a diversidade de sistemas de comunicação sem-fio cooperativos sujeitos a falhas (apagamentos) nos canais interusuário.

Quando um código MDS $\mathcal{C}$ tem um conjunto de elementos de sua matriz $\mathbf{P}$ substituído por zeros, o novo código $\mathcal{C}'$ certamente não é mais MDS. Seja $A = \{(a_1, b_1), (a_2, b_2), ...\}$ um subconjunto de elementos de $\mathbf{P}$ que tenham sido substituídos por zeros. O subconjunto A é reconhecido como uma *falha*. Seja $\mathcal{A} = \{A_0, A_1, \ldots, A_{f-1}\}$ uma coleção de f falhas. Considera-se que duas falhas distintas A_i e A_j não podem conter nenhum elemento da matriz $\mathbf{P}$ em comum. Isso é, $A_i \cap A_j = \emptyset$. Também é considerado que cada falha possui cardinalidade fixa, isto é, $|A_i| = |A| \ \forall i$. Embora estas considerações possam parecer muito restritivas, ficará evidente que elas são suficientes para o propósito de solucionar nosso problema principal.

Seja $\chi = (\chi_0, \ldots, \chi_{f-1})$ um indicador binário associado à ocorrência de falhas, ou seja

$$\begin{cases} \chi_i = 1 & \text{caso } A_i \text{ ocorra} \\ \chi_i = 0 & \text{caso } A_i \text{ não ocorra.} \end{cases}$$

Para um inteiro não-negativo i', seja $b(i')$ a representação binária (em forma de vetor) de i'. A coleção de todas as possíveis combinações de falhas é denominada $\mathcal{B} = \{B_{b(0)}, B_{b(1)}, ..., B_{b(2^f-1)}\}$, com $B_\chi = \{(a,b) | (a,b) \in \bigcup_{i:\chi_i=1} A_i\}$, em que (a, b) representa uma entrada (ou um elemento) da matrix $\mathbf{P}$. Para facilitar o entendimento, considere o seguinte exemplo:

Exemplo 5.2 *Seja a matriz apresentada em* (5.10) *para o caso especial em que* $k = 4$ *e* $n = 8$. *A matriz de paridade* $\mathbf{P}$ *teria a forma:*

$$\mathbf{P} = \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & p_{1,4} \\ p_{2,1} & p_{2,2} & p_{2,3} & p_{2,4} \\ p_{3,1} & p_{3,2} & p_{3,3} & p_{3,4} \\ p_{4,1} & p_{4,2} & p_{4,3} & p_{4,4} \end{bmatrix}.$$

Supõe-se agora que $\mathbf{P}$ *esteja sujeita a falhas nas seguintes posições:*

$A_0 = \{(3,1),(3,2)\}$, $A_1 = \{(4,1),(4,2)\}$, $A_2 = \{(1,3),(1,4)\}$ *e* $A_3 = \{(2,3),(2,4)\}$, *ou seja, o número total de falhas a que* $\mathbf{P}$ *está sujeita é* $f = 4$, *resultando em* $2^4 = 16$ *combinações distintas. O número de elementos substituídos por zero na ocorrência de cada falha é* $|A| = 2$. *Para uma dada realização de canal, considere que somente as falhas* A_0 *e* A_3 *tenham realmente ocorrido. Neste caso, a matriz* $\mathbf{P}'$ *resultante teria a forma*

$$\mathbf{P}' = \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & p_{1,4} \\ p_{2,1} & p_{2,2} & 0 & 0 \\ 0 & 0 & p_{3,3} & p_{3,4} \\ p_{4,1} & p_{4,2} & p_{4,3} & p_{4,4} \end{bmatrix}.$$

Nesta situação, tem-se que $\chi_0 = 1$, $\chi_1 = 0$, $\chi_2 = 0$ *e* $\chi_3 = 1$, *levando a* $b(i') = 1001$. *Ou seja, para este evento tem-se que* $B_\chi = \{(3,1),(3,2),(2,3),(2,4)\}$, *correspondendo aos índices de todos os elementos que foram substituídos por zero.*

Cada evento B_χ, o qual consiste da ocorrência de $|B_\chi|/|A|$ falhas, dá origem a um código de bloco $\mathcal{C}(B_\chi)$ com distância mínima de Hamming $d_{min}(\mathcal{C}(B_\chi))$. A denominada *distância mínima composta* do código $\mathcal{C}(B_\chi)$ é aqui definida como

$$d_{min}^{\text{comp}}(\mathcal{C}(B_\chi)) \triangleq d_{min}(\mathcal{C}(B_\chi)) + |B_\chi|/|A|, \tag{5.11}$$

a qual é composta pela distância mínima de Hamming $d_{min}(\mathcal{C}(B_\chi))$ mais um termo de "compensação" relacionado ao número de falhas e à probabilidade de ocorrência da combinação B_χ. Em outras palavras, este termo compensa a probabilidade (baixa) de que o código tenha a sua distância minima reduzida para $d_{min}(\mathcal{C}(B_\chi))$, e fundamenta-se na analogia entre distância mínima e ordem de diversidade.

Um parâmetro de fundamental importância para indicar o desempenho de um código MDS sujeito a um codificador com falhas é a sua *menor distância mínima composta* de qualquer combinação possível de falhas. Dado um código MDS $\mathcal{C}$ e uma coleção de f falhas $\mathcal{A}$, essa distância é definida como:

$$d_{min}^{\text{comp}}(\mathcal{C},\mathcal{A}) \triangleq \min_{B_\chi \in \mathcal{B}} \left\{ d_{min}^{\text{comp}}(\mathcal{C}(B_\chi)) \right\}, \tag{5.12}$$

em que, para não haver confusão, ela é simplesmente chamada *distância mínima composta*.

No que se segue, uma sequência de resultados que constituem a teoria de matrizes geradoras deficientes será provada.

Lema 5.2 *A distância de Hamming entre duas palavras-código y e z é limitada inferiormente pela diferença entre seus pesos individuais,* i.e., $w(y \boxplus z) \geq |w(y) - w(z)|$.

Prova: A partir da desigualdade triangular (Seção 2.1), $w(y' \boxplus z') \leq w(y') + w(z')$. Se selecionarmos $y' = y \boxplus z$ e $z' = \boxminus z$, em que $\boxminus z$ é o inverso aditivo de z, obtemos $w(y \boxplus z) \geq |w(y) - w(z)|$, provando o lema. □

Teorema 5.3 *Seja $\mathcal{C}$ um código MDS (n, k, d_{min}) com matriz geradora na forma sistemática $\boldsymbol{G} = [\boldsymbol{I}|\boldsymbol{P}]$. A substituição por zeros de δ elementos em qualquer linha particular de sua matriz $\boldsymbol{P}$ origina um código $(n, k, d_{min} - \delta)$ $\mathcal{C}'$.*

Prova: Sejam $\mathbf{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$ e $\mathbf{G}' = \{\mathbf{g}'_1, \ldots, \mathbf{g}'_k\}$ as matrizes geradoras de $\mathcal{C}$ e $\mathcal{C}'$, respectivamente, com $\mathbf{g}_i$ ($\mathbf{g}'_i$) sendo a i-ésima linha de $\mathbf{G}$ ($\mathbf{G}'$). Sem perda de generalidade, assume-se que δ elementos da parte de paridade da linha $\mathbf{g}_{i^*}$ são substituídos por zeros. Para uma mensagem de informação não-nula $\mathbf{u} = \{u_1, \ldots, u_k\}$, o peso de Hamming da palavra-código não-nula $\mathbf{v}'$ é

$$\begin{aligned}
w(\mathbf{v}') &= w(\mathbf{u}\mathbf{G}') \\
&= w(u_1\mathbf{g}'_1 \boxplus \ldots \boxplus u_{i^*}\mathbf{g}'_{i^*} \boxplus \ldots \boxplus u_k\mathbf{g}'_k) \\
&\overset{(a)}{=} w(u_1\mathbf{g}_1 \boxplus \ldots \boxplus u_{i^*}\mathbf{g}'_{i^*} \boxplus \ldots \boxplus u_k\mathbf{g}_k \boxplus u_{i^*}\mathbf{g}_{i^*} \boxminus u_{i^*}\mathbf{g}_{i^*}) \\
&\overset{(b)}{\geq} w(u_1\mathbf{g}_1 \boxplus \ldots \boxplus u_k\mathbf{g}_k) - w(u_{i^*}\mathbf{g}'_{i^*} \boxminus u_{i^*}\mathbf{g}_{i^*}) \\
&\overset{(c)}{\geq} (n - k + 1) - \delta,
\end{aligned}$$

em que (a) segue do fato de que $\mathbf{g}_i = \mathbf{g}'_i \; \forall i \neq i^*$, (b) segue do Lema 5.2, and (c) segue do limitante de Singleton. Sem perda de generalidade, assume-se que δ elementos da parte de paridade de $\mathbf{g}_{i^*}$ são substituídos por zero, gerando $\mathbf{g}'_{i^*}$, uma palavra-código de $\mathcal{C}'$ com peso $n-k+1-\delta$. O teorema está provado. □

Lema 5.3 *Seja $\mathcal{C}'$ um código $(n, k, n-k-\delta+1)$, com matriz geradora $\boldsymbol{G}' = [\boldsymbol{I}|\boldsymbol{P}']$, obtido a partir de um código MDS $\mathcal{C}$ de acordo com o Teorema 5.3. A substituição por zeros de elementos adicionais em qualquer uma das δ colunas de $\boldsymbol{P}'$ em que outros zeros haviam sido previamente inseridos dá origem a um código $\mathcal{C}''$ com a mesma distância mínima de Hamming que $\mathcal{C}'$.*

Prova: Cada palavra-código de $\mathcal{C}''$ pode ser obtida a partir de uma palavra-código de $\mathcal{C}$ através da mudança de δ posições, as quais são fixas para todas as palavras-código. Assim sendo, deve-se obter $d_{min}(\mathcal{C}'') \geq d_{min}(\mathcal{C}) - \delta$. Como $\mathbf{g}'_{i^*}$, uma palavra-código de $\mathcal{C}'$ com peso de Hamming $n-k-\delta+1$, é também uma palavra-código de $\mathcal{C}''$, o lema está provado. □

Lema 5.4 *Se $\mathcal{C}$ é um código MDS (n, k, d_{min}) com matriz geradora na forma sistemática dada por $\boldsymbol{G} = [\boldsymbol{I}|\boldsymbol{P}]$, a substituição por zeros de δ elementos arbitrários de sua matriz $\boldsymbol{P}$ gera um código $\mathcal{C}'$ com distância mínima de Hamming $d_{min}(\mathcal{C}') \geq d_{min} - \delta$.*

Prova: Similar ao Lema 5.3, com igualdade se o novo código $\mathcal{C}'$ possuir alguma palavra-código com peso de Hamming $d_{min} - \delta$. Por exemplo, se todas as δ substituições ocorrerem em uma única linha de $\mathbf{P}$. □

De acordo com o Lema 5.4, uma única falha A (restrita à matriz $\mathbf{P}$) é capaz de reduzir a distância mínima de Hamming do código MDS original de no máximo $|A|$. Por outro lado, o Teorema 5.3 nos mostra que o pior cenário para uma única falha A é quando todas seus elementos pertencem a uma única linha de $\mathbf{P}$. O último resultado desta seção se refere ao pior caso para uma coleção de falhas.

Lema 5.5 *Seja $\mathcal{C}$ um código MDS (n, k, d_{min}) com matriz geradora na forma sistemática dada por $\boldsymbol{G} = [\boldsymbol{I}|\boldsymbol{P}]$. Considere uma coleção $\mathcal{A} = \{A_0, A_1, \ldots, A_{f-1}\}$ de f falhas, em que $|A_i| = |A| \geq 1$, $\forall i$. Se todas as falhas ocorrem em uma única linha de $\boldsymbol{P}$, então a distância mínima composta de $\mathcal{C}$ sujeita a $\mathcal{A}$ é uma função monotonicamente decrescente do número de falhas.*

Prova: A partir do Teorema 5.3, cada falha reduz a distância mínima de Hamming de exatamente $|A| \geq 1$, e contribui somente com 1 para o termo de "compensação" da distância mínima composta. No caso especial em que $|A| = 1$, a distância mínima composta de $\mathcal{C}$ é constante independentemente do número de falhas. □

5.3.2 GDNC com Máxima Diversidade

Relembrando, o problema em questão é projetar um código de rede linear para o esquema GDNC tal que, dados todos os padrões de erro nos canais interusuário e levando em consideração suas probabilidades de ocorrência, assegure que a diversidade seja $M + k_2$. A solução deste problema é apresentada na sequência.

Teorema 5.4 *Se uma matriz geradora sistemática de um código MDS $\mathcal{C}$ com distância mínima $d_{min} = Mk_2 + 1$ é usada como matriz de transferência do esquema GDNC, a diversidade $D_{GDNC} = M + k_2$ é garantida.*

Prova: Relacionando o problema em questão com o da Seção 5.3.1, uma falha corresponde a um canal interusuário estando em *outage*. Quando isso ocorre, o usuário não é capaz de decodificar corretamente a informação de seu parceiro. Assim sendo, na formação das k_2 combinações lineares para gerar seus k_2 pacotes de paridade, este usuário considera a mensagem erroneamente decodificada como sendo um pacote composto somente por zeros ou, equivalentemente, ajusta para zero os k_2 coeficientes associados a este parceiro. Essa ação corresponde à substituição das k_2 correspondente posições da matriz de paridade $\mathbf{P}$ por zeros, *i.e.*, $|A| = k_2$. Como cada usuário conhece sua própria informação, k_2 elementos de cada linha de $\mathbf{P}$ são imunes a falhas, enquanto as outras $k_2(M-1)$ entradas são sujeitas a falhas. No pior cenário, quando todas as falhas possíveis acontecem, a matriz geradora se torna

$$\mathbf{G} = \left[\begin{array}{c|ccc} & P_1 & & \\ I & & \ddots & \\ & & & P_M \end{array}\right], \tag{5.13}$$

em que cada submatriz P_i de dimensões $(k_1 \times k_2)$ contém os elementos imunes associados ao usuário i. A partir do Teorema 5.2, sabe-se que cada submatriz de P_i é não-singular. Então, a menor distância mínima de Hamming de um código de bloco obtido de um código MDS original $\mathcal{C}$ devido à ocorrência de falhas é $k_2 + 1$. Todavia, a mesma distância mínima pode ser obtida com um número muito menor de falhas. Partindo do Lema 5.3 e do Teorema 5.3, pode-se ver que o número mínimo de falhas capaz de gerar um código com distância mínima $k_2 + 1$ é $M - 1$, quando todas essas falhas ocorrem na mesma linha de $\mathbf{P}$, por exemplo.

Para todas as mínimas distâncias possíveis na faixa $k_2 + 1 \leq d_{min} \leq Mk_2 + 1$, uma condição suficiente para o pior cenário possível (o menor número de falhas que resulta nesta distância mínima) é quando todas as falhas estão localizadas na mesma linha de $\mathbf{P}$, de acordo com o Lema 5.4. Assim sendo, a partir do Lema 5.5, pode-se notar que quanto maior o número de falhas em uma dada linha (e consequentemente a menor distância mínima do código resultando), menor a distância mínima composta. Isso assegura que o código com distância mínima $k_2 + 1$

é o código que gera a menor distância mínima composta, a qual é então dada por

$$\begin{aligned} d_{min}^{\text{comp}} &= \min_{B_\chi \in \mathcal{B}} \{d_{min}(\mathcal{C}(B_\chi)) + |B_\chi|/|A|\} \\ &= (k_2 + 1) + (M - 1) \\ &= M + k_2 \end{aligned} \tag{5.14}$$

É fácil de se notar a conexão entre os dois termos da distância mínima composta e os expoentes de P_e em (5.7c) e (5.9a). Dessa forma, a prova agora está completa □

Teorema 5.5 *Se uma matriz geradora de um código não-MDS é usada como a matriz de transferência no esquema GDNC, a diversidade máxima apresentada no Teorema 5.1 não é garantida.*

Prova: Seja $\mathcal{C}$ um código MDS (n, k, d_{min}) com matriz geradora na forma sistemática dada por $\mathbf{G} = [\mathbf{I}|\mathbf{P}]$. Substituindo um (ou mais) elemento(s) de sua matriz $\mathbf{P}$ por zero(s) origina um código $\mathcal{C}'$ com distância mínima $d'_{min} < d_{min}$, de acordo com o Teorema 5.3. Se o(s) elemento(s) substituído(s) por zero(s) pertencer(em) aos elementos que são imunes a falhas, pode-se facilmente mostrar que há um padrão de $M - 1$ falhas que gera uma palavra-código de peso menor que $k_2 + 1$. Assim sendo, a distância mínima composta seria no máximo $d_{min}^{\text{comp}} = M + k_2 - 1$, de acordo com (5.12). □

Provado que códigos MDS são suficientes e necessários para garantir a diversidade máxima do esquema GDNC, o problema do projeto do código de rede é reduzido a um projeto de código MDS, sem a necessidade de testar uma grande quantidade de códigos de rede distintos, levando em consideração todos os padrões de erro nos canais interusuário, e os seus impactos na diversidade do sistema. A classe de códigos MDS bem difundida na literatura chamada Reed-Solomon (RS) [44, Cap.3] [36, Cap.10], por exemplo, pode ser utilizada[4]. No nó destino, os pacotes de mensagens dos diversos usuários podem ser

[4]A matriz geradora de um código $(n, k, n - k + 1)$ RS (ou RS estendido) sobre GF(q) na sua forma sistemática pode ser facilmente obtida com o aplicativo SAGE [71], através do seguinte código:

```
F.<alpha> = GF(q)
C = ReedSolomonCode(n,k,F)
G = C.gen_mat()
show(G.echelon_form())
```

recuperados através de algum decodificador clássico de códigos RS, por exemplo [11, 12].

Deve-se notar que o tamanho do campo q deve ser grande o suficiente para que o código RS exista [36, Cap.11, Coroll.7]. A este respeito, o seguinte resultado é apresentado:

Teorema 5.6 *Existe um código MDS com* $(n = M(k_1 + k_2), k = Mk_1, d_{min} = Mk_2 + 1)$ *sobre GF(q) (em que q é uma potência de um número primo) que pode servir a um sistema GDNC atingindo máxima diversidade* $M + k_2$ *se* $q \geq M(k_1 + k_2)$.

Prova: Queremos encontrar um código MDS com $(n = M(k_1+k_2), k = Mk_1, d_{min} = Mk_2+1)$ sobre GF(q). Iniciemos escolhendo um tamanho de campo $q \geq M(k_1+k_2)$ como uma potência de um número primo. De acordo com [36], existe um código RS com $(n' = q-1, k' = Mk_1, d'_{min} = q-Mk_1)$ sobre GF(q). Se $q = M(k_1+k_2)+1$, o código RS é simplesmente utilizado como o código MDS. Se $q = M(k_1 + k_2)$, podemos adicionar um símbolo de paridade e ter um código RS estendido com $(q, Mk_1, q - Mk_1 + 1)$ sobre GF(q), o qual pode ser usado como o código MDS. No caso em que $q > M(k_1 + k_2) + 1$, então podemos puncionar o código RS em exatamente $q - M(k_1 + k_2) - 1$ posições, resultando em um código com $(n = M(k_1 + k_2), k = Mk_1, d_{min} = Mk_2 + 1)$, o qual é MDS. □

Uma comparação entre o tamanho do campo finito necessário para que a ordem de diversidade completa seja atingida nos esquemas GDNC (de acordo com o limitante apresentado no Teorema 5.6) e no esquema DNC simplificado (de acordo com a estimativa apresentada em [69] e reproduzida em (4.11)) está apresentada na Tabela 5.1.

Tabela 5.1: Tamanho de campo necessário para que a diversidade proposta nos esquemas GDNC (com $k_1 = 1$ e $k_2 = M - 1$) e DNC simplificado sejam atingidas.

M	2	3	4	5
$q_{\min}$(GDNC)	4	9	16	25
$q_{\min}$(DNC)	3	28	455	10626

Ressalta-se que os valores apresentados na Tabela 5.1 para o esquema DNC correspondem ao valor do campo finito necessário para que a diversidade $2M - 1$ seja atingida, de acordo com a estimativa apresentada por Xiao em [69]. Porém, como o esquema GDNC com parâmetros com $k_1 = 1$ e $k_2 = M - 1$ se reduz ao esquema DNC, essa

diversidade pode ser atingida com um valor de campo finito bem menor, como apresentado na Tabela 5.1.

As Tabelas 5.2 e 5.3 apresentam a matriz de paridade $\mathbf{P}$, descrita em (5.10), de alguns códigos MDS obtidos a partir de códigos RS (conforme explicado na prova do Teorema 5.6) os quais podem ser utilizados como a matriz de transferência da rede, para $M = 2$ e $M = 3$ usuários, respectivamente. Estas matrizes foram obtidas utilizando o software SAGE [71].

Tabela 5.2: Códigos de rede obtidos de códigos RS para rede com 2 usuários.

k_1	k_2	Taxa	Campo q	Matriz de paridade $\mathbf{P}$
1	1	2/4	4	$\begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}$
1	2	2/6	8	$\begin{bmatrix} 3 & 5 & 1 & 7 \\ 2 & 4 & 3 & 6 \end{bmatrix}$
2	1	4/6	8	Obtido a partir do código 4/8 puncionando-se as 2 últimas colunas
2	2	4/8	8	$\begin{bmatrix} 3 & 7 & 3 & 6 \\ 5 & 7 & 7 & 4 \\ 2 & 4 & 6 & 1 \\ 5 & 5 & 3 & 2 \end{bmatrix}$
2	3	4/10	16	Obtido a partir do código 4/12 puncionando-se as 2 últimas colunas
2	4	4/12	16	$\begin{bmatrix} 14 & 5 & 7 & 10 & 4 & 10 & 8 & 9 \\ 12 & 4 & 14 & 5 & 12 & 12 & 14 & 7 \\ 13 & 6 & 12 & 15 & 8 & 1 & 4 & 10 \\ 14 & 6 & 4 & 1 & 1 & 6 & 3 & 5 \end{bmatrix}$
3	2	6/10	16	Obtido a partir do código 6/12 puncionando-se as 2 últimas colunas
3	3	6/12	16	$\begin{bmatrix} 11 & 2 & 4 & 6 & 14 & 12 \\ 1 & 11 & 13 & 10 & 14 & 10 \\ 2 & 4 & 2 & 10 & 5 & 9 \\ 6 & 13 & 12 & 11 & 8 & 12 \\ 4 & 12 & 12 & 2 & 6 & 6 \\ 11 & 13 & 10 & 14 & 10 & 4 \end{bmatrix}$

Tabela 5.3: Códigos de rede obtidos a partir códigos RS para rede com 3 usuários.

k_1	k_2	Taxa	Campo q	Matriz de paridade $\mathbf{P}$
1	1	3/6	8	$\begin{bmatrix} 4 & 1 & 5 \\ 3 & 1 & 3 \\ 6 & 1 & 7 \end{bmatrix}$
2	1	6/9	16	Obtido a partir do código 6/12 puncionando-se as 3 últimas colunas
1	2	3/9	16	$\begin{bmatrix} 15 & 11 & 1 & 14 & 5 & 11 \\ 8 & 5 & 1 & 8 & 13 & 4 \\ 6 & 15 & 1 & 7 & 9 & 14 \end{bmatrix}$
2	2	6/12	16	$\begin{bmatrix} 11 & 2 & 4 & 6 & 14 & 12 \\ 1 & 11 & 13 & 10 & 14 & 10 \\ 2 & 4 & 2 & 10 & 5 & 9 \\ 6 & 13 & 12 & 11 & 8 & 12 \\ 4 & 12 & 12 & 2 & 6 & 6 \\ 11 & 13 & 10 & 14 & 10 & 4 \end{bmatrix}$

5.4 Simulações

5.4.1 Cálculo da Taxa de Apagamento de Pacote (FER)

Ao representar a topologia da rede em forma de uma matriz sistemática, de acordo com o apresentado na Seção 5.3, o acontecimento de falhas nos canais interusuário faz com que certas posições da parte da paridade desta matriz possuam uma probabilidade não nula de serem substituídas por zero. Além das falhas (*outages*) nos canais interusuário, ainda há a possibilidade de ocorrência de falhas nos canais entre os usuários e a ERB, o que resultaria em um apagamento de uma coluna completa da matriz.

Em suma, as falhas podem ocorrer tanto nos enlaces interusuário quanto nos enlaces entre os usuários e a ERB.

5.4.2 Posto de uma Matriz

O posto (em inglês *rank*) de uma matriz $\mathbf{G}$ corresponde à quantidade máxima de linhas/colunas linearmente independentes que a mesma possui. A respeito do posto, é verdade que [72]:

(i) O posto de uma matriz de dimensões $m \times n$ é no máximo $\min(m, n)$;

(ii) Uma matriz que possui o maior posto possível é dita ter posto completo, caso contrário, terá posto deficiente.

Aplicando o conceito de posto ao problema em questão, caso a matriz de transferência $\mathbf{G}$ tenha posto completo, então todas as variáveis[5] podem ser recuperadas com sucesso.

A taxa de apagamento de pacote será calculada com base no posto da matriz recebida na ERB após a ocorrência de todas as possíveis falhas. Seja $\mathbf{G}$ a matriz que representa o código de rede original (antes da ocorrência de falhas) e $\mathbf{G}' = \left[\mathbf{I}'|\mathbf{P}'\right]$ a matriz resultante após a ocorrência de todas as falhas. A quantidade de pacotes de informação não recuperados pela ERB após a rodada de transmissão[6] τ é considerada como sendo

$$N_e(\tau) = \begin{cases} 0, & \text{se posto}(\mathbf{G}) = \text{posto}(\mathbf{G}') \\ \text{posto}(\mathbf{G}) - \text{posto}(\mathbf{I}'), & \text{caso contrário} \end{cases} \tag{5.15}$$

Ressalta-se que o procedimento utilizado em (5.15) é um limitante superior para o número de apagamentos de pacotes, o qual foi verificado através de simulações ser muito próximo ao valor exato, e foi assim adotado a fim de reduzir a complexidade das simulações. A taxa de apagamento[7] de pacote (FER, do inglês *frame erasure rate*) é finalmente definida como:

$$\text{FER} = \frac{1}{Mk_1T}\sum_{\tau=1}^{T} N_e(\tau), \tag{5.16}$$

em que T é o número total de rodadas de transmissão.

5.4.3 Resultado das Simulações

Nas simulações, foi considerado que a taxa de informação de cada enlace é de $R = 0.5$ bits/uso do canal. Ressaltando que a ordem de diversidade não depende do valor de R, como mostrado na Seção 4.1.2.

A Figura 5.3 apresenta a FER em função da SNR para uma rede com 2 usuários, considerando os esquemas BNC, DNC (Figura 4.4) sobre GF(4), e o proposto GDNC com $k_1 = k_2 = 2$ sobre GF(8), com a matriz geradora obtida da Tabela 5.2, todos os três esquemas com a mesma taxa 1/2. Com respeito à probabilidade de *outage* analítica, considera-se o limitante superior, o qual foi obtido através da substituição do limitante

[5] As variáveis neste contexto são definidas como os pacotes de informação transmitidos pelos M usuários durante a fase de difusão, os quais também estão contidos nos pacotes de verificação de paridade transmitidos durante a fase de cooperação.

[6] Uma rodada de transmissão é composta por uma fase de difusão mais uma fase de cooperação.

[7] A rigor, trata-se de uma taxa de insucesso de decodificação, visto que reflete a taxa dos pacotes que não foram corretamente recuperados pela ERB.

superior de $\gamma(k_1, k_2, \overline{D}_{j,t})$ de (5.8) em (5.9). Como esperado, o esquema proposto atinge uma ordem de diversidade maior que a dos outros dois esquemas com a mesma taxa. A diferença entre os valores analíticos e os obtidos através de simulações ocorre devido ao uso do limitante superior mencionado anteriormente. Todavia, pode-se perceber que a ordem de diversidade obtida através de simulações condiz com a obtida analiticamente.

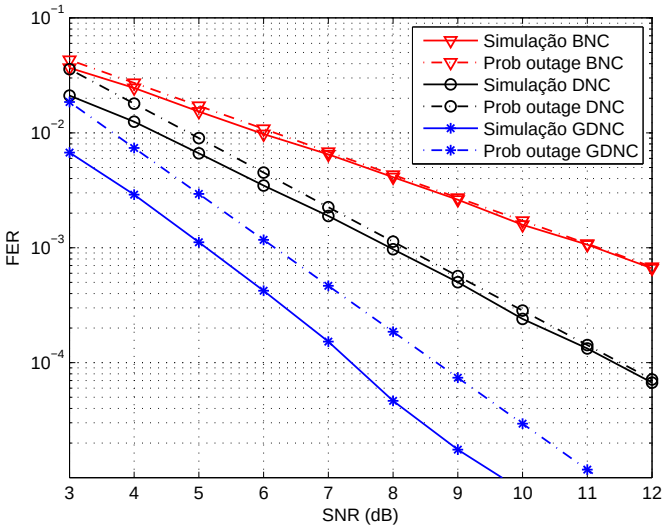


Figura 5.3: FER versus SNR (dB) para um sistema com 2 usuários e taxa $R = 1/2$, considerando os esquemas BNC, DNC (sobre GF(4), de acordo com (5.10)) e o proposto GDNC (com $k_1 = k_2 = 2$ e sobre GF(8), de acordo com a Tabela 5.2).

Deve-se mencionar que, como a máxima ordem de diversidade 3 do esquema DNC já é atingida com o campo GF(4), aumentar o tamanho do campo não traria nenhum benefício adicional neste caso. Por outro lado, como discutido no início deste capítulo, para o esquema GDNC usado nas simulações, o qual corresponde a um código de bloco de taxa 4/8, um campo de tamanho 8 é necessário para atingir $d_{min} = 5$. Deve-se também ressaltar que no esquema proposto, somente as combinações lineares são realizadas sobre GF(q); o esquema de modulação e o modo de transmissão são irrelevantes para o funcionamento do GDNC, e podem ser o mesmo para todos os esquemas.

A Figura 5.4 mostra o desempenho em termos de FER para o esquema GDNC proposto ilustrado na Figura 5.3, bem como para outros dois esquemas GDNC cujas matrizes de transferência utilizadas correspondem às matrizes geradores de códigos não-MDS (geradas aleatoriamente e apresentadas na Tabela 5.4) com os mesmos parâmetros $k_1 = k_2 = 2$ e taxa 1/2, mas com distância mínima 3 e 4. Pode-se ver que, com $d_{min} = 3$, a ordem de diversidade é somente

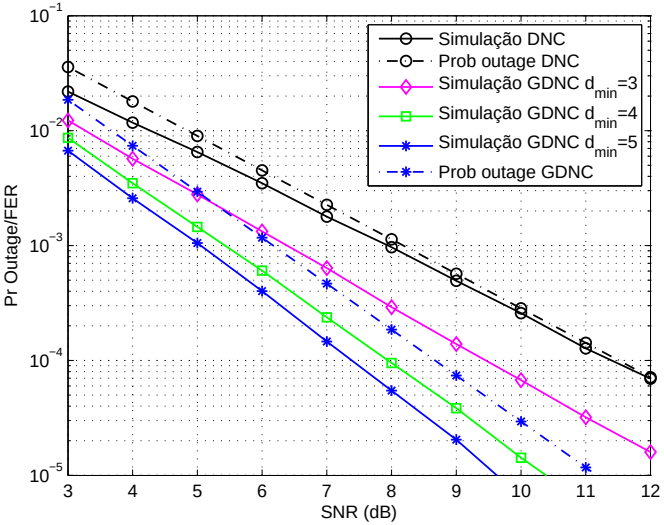


Figura 5.4: FER versus SNR (dB) para um sistema com 2 usuários e taxa $R = 1/2$, considerando os esquemas BNC, DNC (sobre GF(4), de acordo com (5.10)) e o proposto GDNC (com $k_1 = k_2 = 2$ e sobre GF(8), de acordo com as Tabelas 5.2 e 5.4).

3, enquanto com $d_{min} = 4$ a ordem de diversidade é muito próxima à obtida com o código MDS (com $d_{min} = 5$). Neste caso, um código quase-MDS é capaz de praticamente atingir a diversidade máxima.

Todavia, na Figura 5.5, um código diferente, também com $d_{min} = 4$ (dado na Tabela 5.4), é mostrado não atingir a diversidade máxima. Assim sendo, podemos ver que ao considerar como matriz de transferência a matriz geradora de um código quase-MDS, a ordem de diversidade $M + k_2$ não é garantida, de acordo com o apresentado no Teorema 5.5.

Tabela 5.4: Códigos de rede obtidos a partir de códigos de bloco com distância mínima 3 e 4.

Fig.	d_{min}	Matriz de paridade $\mathbf{P}$
5.4 e 5.5	3	$\begin{bmatrix} 0 & 5 & 5 & 3 \\ 4 & 7 & 7 & 1 \\ 7 & 7 & 7 & 1 \\ 7 & 2 & 3 & 7 \end{bmatrix}$
5.4	4	$\begin{bmatrix} 4 & 2 & 5 & 3 \\ 5 & 4 & 6 & 4 \\ 7 & 6 & 1 & 4 \\ 1 & 1 & 3 & 1 \end{bmatrix}$
5.5	4	$\begin{bmatrix} 0 & 5 & 5 & 5 \\ 7 & 4 & 6 & 3 \\ 7 & 0 & 4 & 7 \\ 2 & 7 & 6 & 0 \end{bmatrix}$

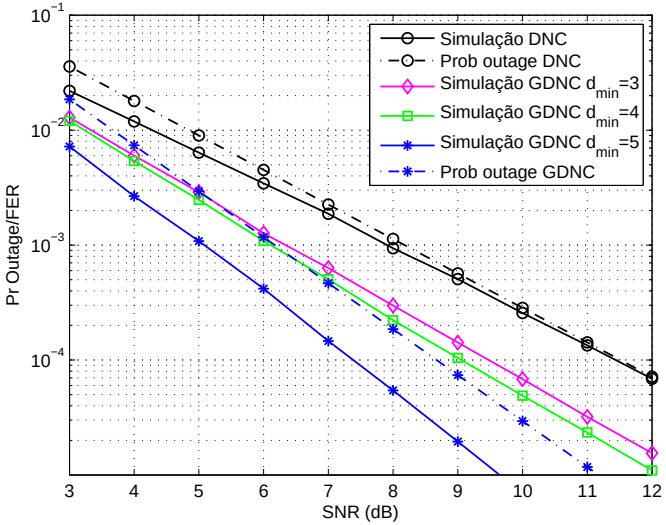


Figura 5.5: FER versus SNR (dB) para um sistema com 2 usuários e taxa $R = 1/2$, considerando os esquemas BNC, DNC (sobre GF(4), de acordo com (5.10)) e o proposto GDNC (com $k_1 = k_2 = 2$ e sobre GF(8), de acordo com as Tabelas 5.2 e 5.4).

5.5 Comentários

Neste capítulo, uma nova abordagem de projeto de códigos de rede para redes cooperativas de múltiplo acesso sujeitas a falhas nos enlaces interusuário foi proposta. O esquema proposto, denominado codificação de rede dinâmica generalizada (GDNC), faz uso de conceitos da teoria de codificação clássica no projeto de códigos de rede com o intuito de melhorar o desempenho de erro da rede. Mostrou-se que a ordem de diversidade do sistema está diretamente relacionada ao tamanho do código utilizado (através da utilização do limitante de Singleton como um limitante para a ordem de diversidade), bem como à necessidade de um campo finito suficientemente grande capaz de atingir a máxima distância mínima.

No esquema GDNC, a ordem de diversidade e/ou a taxa de transmissão podem ser aumentadas se comparadas ao esquema DNC proposto em [18]. Porém, uma possível desvantagem do esquema GDNC em comparação ao DNC deve ser ressaltada: Devido ao código de rede apresentar dimensões maiores, o atraso de transmissão[8] no esquema GDNC pode ser maior que no esquema DNC. No esquema DNC, após a transmissão da primeira mensagem de informação da fase de difusão, a mesma só estará disponível na ERB após $(M-1)+M(M-1)$ instantes de transmissão. No esquema GDNC, a mesma informação estará disponível após k_1M-1+k_2M instantes de transmissão.

No próximo capítulo, elaborar-se-á sobre o esquema GDNC apresentado neste capítulo através da suposição de existência de um canal de retorno entre a ERB e os usuários, o qual auxiliará a aumentar ainda mais a taxa do sistema, sem reduzir a ordem de diversidade.

[8]Tempo entre o instante de transmissão e o instante em que todas as paridades são recebidas na ERB, sem levar em conta o tempo necessário para a decodificação.

Capítulo 6

GDNC com Canal de Retorno

EM ambos os esquemas DNC e GDNC, uma vez que o código de rede é projetado, este permanece o mesmo até que ocorra uma alteração na topologia da rede (tal como mudança no número de usuários) e um novo código seja requisitado. Porém, tal característica tem um impacto maléfico na taxa do sistema: À medida que a SNR aumenta, a probabilidade de que a ERB decodifique corretamente toda a informação recebida durante a fase de difusão também aumenta. Nesse caso, a transmissão de pacotes de paridade não seria mais necessária.

Como o número de pacotes de informação transmitidos durante a fase de difusão no esquema GDNC é igual a Mk_1, a probabilidade de todos estes pacotes serem corretamente decodificados é dada por

$$\Pr\{\text{Nenhum em } \textit{outage}\} = (1 - P_e)^{Mk_1}, \tag{6.1}$$

em que P_e é a probabilidade de *outage* de um enlace individual, dada em (4.4) para desvanecimento Rayleigh.

O aumento da probabilidade em (6.1) com a SNR é ilustrado na Figura 6.1, para uma rede com 2 usuários com $k_1 = 2$.

Para SNR= 12dB, por exemplo, a probabilidade de que nenhum enlace esteja em *outage* é aproximadamente $0,9$, o que significa que em 90% do tempo pacotes de verificação de paridade desnecessários estão sendo transmitidos, comprometendo a taxa do sistema.

Neste capítulo, uma alteração para o esquema GDNC apresentado no Capítulo 5 é proposta, com o intuito de se evitar esse desperdício na taxa do sistema, sem comprometer a sua ordem de diversidade. O esquema aqui proposto é baseado na suposição de que existe um

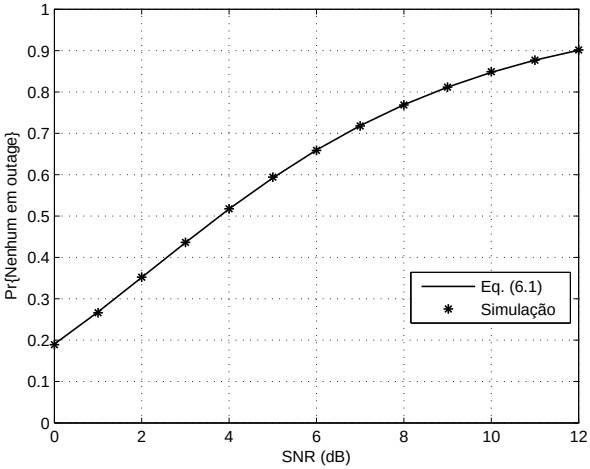


Figura 6.1: Probabilidade de todos os pacotes de informação transmitidos durante a fase de difusão serem decodificados corretamente na ERB versus a SNR, para uma rede com $M = 2$ usuários e parâmetro $k_1 = 2$.

canal de retorno entre a ERB e os usuários, livre de erros, pelo qual os usuários são informados sobre o sucesso/falha na decodificação dos pacotes transmitidos durante a fase de difusão. Cada mensagem transmitida pela ERB é composta por somente um bit, chamado *bit de outage* (OUT). OUT = 0 significa que a ERB decodificou corretamente determinado pacote de informação (ou um conjunto de pacotes de informação), e OUT = 1 significa que o pacote de informação (ou parte de um conjunto de pacotes) não foi corretamente decodificado.

Dependendo de quando os bits de OUT são enviados, como também da quantidade de bits de OUT enviados, diferente abordagens podem ser consideradas. No que se segue, duas abordagens que requerem diferentes quantidades de *feedback* são propostas.

6.1 Abordagem 1

Nesta primeira abordagem, a ERB envia um bit de OUT após cada fase de difusão. Se esse bit for igual a 0, significa que todos os Mk_1 pacotes de informação recebidos anteriormente foram corretamente decodificados, e novos pacotes de informação podem ser gerados e transmitidos. De acordo com o apresentado em (6.1), esse evento tem probabilidade $\Pr\{\text{OUT}=0\} = (1 - P_e)^{Mk_1}$. Caso contrário, se um 1 é recebido de volta pelos usuários, significa que pelo menos um dos Mk_1

pacotes de informação não foi decodificado corretamente, o que ocorre com probabilidade $\Pr\{\text{OUT=1}\} = 1 - \Pr\{\text{OUT=0}\}$. Nesse caso, cada usuário transmite k_2 pacotes de paridade, de acordo com o esquema GDNC original apresentado no Capítulo 5, composto de todos os pacotes de informação que ele pôde decodificar corretamente durante a fase de difusão.

6.1.1 Probabilidade de *Outage* e Diversidade

A análise da probabilidade de *outage* para esta primeira abordagem é a mesma apresentada na Seção 5.2. Como todos os usuários transmitem k_2 pacotes de verificação de paridade se qualquer um dos pacotes de informação não for corretamente decodificado pela ERB, a condição necessária para que uma *outage* ocorra é a mesma do esquema GDNC apresentado no capítulo anterior. Isso resulta na mesma probabilidade de *outage* e consequentemente na mesma diversidade $M + k_2$ que em (5.9).

6.1.2 Análise da Taxa

Seja T o número de rodadas de transmissão consideradas[1]. O número de pacotes de informação transmitidos por rodada é sempre $k_1 M$. A taxa instantânea durante a rodada τ é dada por

$$R_{\tau,Ap1} = \frac{Mk_1}{Mk_1 + P_{\tau,Ap1}}, \tag{6.2}$$

em que $P_{\tau,Ap1}$ representa o número de pacotes de verificação de paridade transmitidos na rodada τ, para $\tau = 1, \ldots, T$.

Nesta abordagem, de acordo com o bit retornado pela ERB, existem duas possibilidades para $P_{\tau,Ap1}$:

$$P_{\tau,Ap1} = \begin{cases} 0, & \text{se OUT=0} \\ Mk_2, & \text{se OUT=1,} \end{cases} \tag{6.3}$$

e o seu valor esperado é dado por

$$E\left[P_{\tau,Ap1}\right] = \Pr\{P_{\tau,Ap1}{=}0\}0 + \Pr\{P_{\tau,Ap1}{=}Mk_2\}Mk_2 \tag{6.4a}$$

$$= \overline{P_e}^{Mk_1} 0 + \left(1 - \overline{P_e}^{Mk_1}\right) Mk_2 \tag{6.4b}$$

$$= Mk_2 \left(1 - \overline{P_e}^{Mk_1}\right), \tag{6.4c}$$

[1] Uma rodada de transmissão é composta por uma fase de difusão mais uma fase de cooperação.

em que $\overline{P_e} = 1 - P_e$. O comprimento do bloco na rodada τ é $L_{\tau,Ap1} = Mk_1 + P_{\tau,Ap1}$ pacotes. A taxa total para as T rodadas de transmissão é dada por

$$R_{T,Ap1} = \frac{TMk_1}{\sum_{\tau=1}^{T} L_{\tau,Ap1}} = \frac{Mk_1}{Mk_1 + \frac{1}{T}\sum_{\tau=1}^{T} P_{\tau,Ap1}}, \tag{6.5}$$

a partir da qual finalmente podemos obter a taxa média

$$\begin{aligned} \overline{R}_{Ap1} &= \lim_{T\to\infty} R_{T,Ap1} && \text{(6.6a)} \\ &= \frac{Mk_1}{Mk_1 + E\left[P_{\tau,Ap1}\right]} && \text{(6.6b)} \\ &= \frac{k_1}{k_1 + k_2\left(1 - \overline{P_e}^{Mk_1}\right)}. && \text{(6.6c)} \end{aligned}$$

Pode-se ver em (6.6c) que, como $0 \leq \overline{P_e}^{Mk_1} \leq 1$, $\overline{R}_{Ap1}$ é sempre maior ou igual à taxa do esquema GDNC dada em (5.5).

A partir de (6.6c) pode-se também avaliar o comportamento assintótico de $\overline{R}_{Ap1}$. Com respeito à SNR, à medida que ela aumenta sem limites, pode-se ver que $\overline{R}_{Ap1} \to 1$. Quando a SNR diminui sem limites, tem-se que $\overline{R}_{Ap1} \to \frac{k_1}{k_1+k_2}$. Para uma SNR fixa e com respeito ao número de usuários, quando este aumenta sem limites, pode-se ver a partir de (6.6c) que

$$\lim_{M\to\infty} \overline{R}_{Ap1} = \frac{k_1}{k_1 + k_2}, \tag{6.7}$$

o que significa que, mesmo fazendo uso de um canal de retorno, a taxa média da Abordagem 1 tende para a mesma taxa do esquema GDNC sem canal de retorno à medida em que o número de usuários aumenta.

6.2 Abordagem 2

Com o intuito de superar essa limitação e aumentar a taxa do sistema mesmo quando o número de usuários é grande, nesta segunda abordagem considera-se que a ERB é capaz de enviar um bit de retorno por usuário ao invés de um bit de retorno para cada bloco de M usuários. Seja $\mathrm{OUT}_j(\tau)$ o bit de *outage* relativo ao Usuário j na rodada τ. $\mathrm{OUT}_j(\tau) = 0$ se todos os k_1 pacotes de informação transmitidos pelo Usuário j na rodada τ foram corretamente decodificados pela ERB, e $\mathrm{OUT}_j(\tau) = 1$ caso contrário. Assim sendo, os usuários receberão um conjunto de M bits após cada fase de difusão. Se o tamanho do pacote de informação é grande o suficiente, essa quantidade de informação de

retorno continua sendo desprezível.

Com base na informação de retorno recebida, nesta abordagem cada usuário pode possuir um parâmetro k_2 diferente, o qual é adaptativo e variante no tempo. Seja $k_{2,j}(\tau)$ o parâmetro k_2 do Usuário j na rodada de transmissão τ, definido como

$$k_{2,j}(\tau) = \begin{cases} 0, & \text{se } \sum_{j=1}^{M} \mathrm{OUT}_j(\tau) = 0 \\ k_2, & \text{se } \mathrm{OUT}_j(\tau) \neq 0 \\ k_2', & \text{caso contrário} \end{cases} \tag{6.8}$$

em que k_2 é o mesmo da Abordagem 1.

A primeira linha de (6.8) é equivalente à Abordagem 1: Se todas os Mk_1 pacotes de informação foram decodificados corretamente (a soma de todos os OUTs é igual a zero), então a transmissão de pacotes de verificação de paridade não é mais necessária e $k_{2,j}(\tau)$ é definido como zero para todo j (o que significa que um novo conjunto de Mk_1 pacotes de informação pode ser transmitido). Esse evento tem probabilidade $P_0 = (1 - P_e)^{Mk_1}$, de acordo com (6.1).

Se o Usuário j possuir pelo menos um de seus k_1 pacotes de informação incorretamente decodificado pela ERB, ele irá então definir $k_{2,j}(\tau) = k_2$, o que ocorre com probabilidade $P_{k_2} = 1 - (1 - P_e)^{k_1}$. A principal diferença aqui é quando todos os k_1 pacotes de informação difundidos pelo Usuário j são corretamente decodificados pela ERB, mas pelo menos um dos $(M-1)k_1$ pacotes de informação difundidos pelos outros usuários está em *outage*. Nesse caso, o Usuário j irá colaborar com k_2' pacotes de paridade, em que $0 \leq k_2' \leq k_2$. A questão aqui se resume a descobrir qual o valor de k_2' que maximiza a taxa e que ao mesmo tempo não reduz a ordem de diversidade se comparado ao esquema GDNC original.

6.2.1 Análise da Taxa

Nesta abordagem, a quantidade de pacotes de verificação de paridade transmitida por cada usuário pode ser diferente. Seja $P_{\tau,Ap2}^{j}$ o número de pacotes de verificação de paridade transmitidos pelo Usuário j na rodada τ. De acordo com (6.8), ele pode assumir três diferentes valores.

O número total de pacotes de verificação de paridade transmitidos na rodada τ é dado por

$$P_{\tau,Ap2} = \sum_{j=1}^{M} P_{\tau,Ap2}^{j},$$

resultando no valor esperado

$$\overline{P}_\tau = E\left[\sum_{j=1}^{M} P_\tau^j\right] = ME\left[P_\tau\right] \tag{6.9a}$$

$$= M\sum_{p} \Pr\{P_\tau = p\}\cdot p \tag{6.9b}$$

$$= M\left[\overline{P}_e^{Mk_1}\cdot 0 + (1-\overline{P}_e^{k_1})\cdot k_2 + \left(1-\overline{P}_e^{Mk_1} - (1-\overline{P}_e^{k_1})\right)\cdot k_2'\right] \tag{6.9c}$$

$$= Mk_2 - M\overline{P}_e^{k_1}\left(k_2 - k_2'\left(1-\overline{P}_e^{(M-1)k_1}\right)\right). \tag{6.9d}$$

Por um procedimento similar ao utilizado na Abordagem 1, a taxa média é dada por

$$\overline{R}_{Ap2} = \frac{Mk_1}{Mk_1 + E\left[P_\tau\right]} \tag{6.10a}$$

$$= \frac{k_1}{k_1+k_2-\overline{P}_e^{k_1}\left(k_2 - k_2'\left(1-\overline{P}_e^{(M-1)k_1}\right)\right)}, \tag{6.10b}$$

em que $E\left[P_\tau\right]$ é obtido de (6.9d). Uma vez que $k_2 \geq k_2'$ e $0 \leq \overline{P}_e \leq 1$, pode-se ver a partir de (6.10b) que $\overline{R}_{Ap2} \geq \overline{R}_{GDNC} = \frac{k_1}{k_1+k_2}$.

Com relação ao seu comportamento assintótico, assim como na Abordagem 1, $\overline{R}_{Ap2} \to 1$ quando SNR $\to \infty$ e $\overline{R}_{Ap2} \to \frac{k_1}{k_1+k_2}$ quando SNR $\to -\infty$. Todavia, o comportamento assintótico da taxa com o número de usuários agora é

$$\lim_{M\to\infty} \overline{R}_{Ap2} = \frac{k_1}{k_1 + k_2 - \overline{P}_e^{k_1}\left(k_2 - k_2'\right)}, \tag{6.11}$$

o que assegura que a taxa $\overline{R}_{Ap2}$ é mais alta que a taxa do esquema GDNC apresentado no capítulo anterior mesmo quando o número de usuários cresce sem limites, desde que a condição $k_2 > k_2'$ seja satisfeita.

6.2.2 Probabilidade de *Outage* e Diversidade

Seja $D_{j,t} \subseteq \{1,\ldots,M\}$ o conjunto de índices correspondentes aos usuários que corretamente decodificaram $I_j(t)$, incluindo o próprio índice j, de acordo com a Seção 5.2. A probabilidade de $D_{j,t}$ é dada por

$$P_{D_{j,t}} = P_e^{M-|D_{j,t}|}(1-P_e)^{|D_{j,t}|-1}, \tag{6.12}$$

a qual corresponde à probabilidade de $M-|D_{j,t}|$ dentre os $M-1$ canais interusuário estarem em *outage*.

Também define-se $Q_{j,t} \subset D_{j,t}$ como o conjunto de índices correspondentes aos usuários que corretamente decodificaram $I_j(t)$ e cujos próprios pacotes de informação (todos eles) foram corretamente decodificados pela ERB. Pode-se mostrar que a probabilidade de $Q_{j,t}$ pode ser aproximada como

$$P_{Q_{j,t}} \approx P_e^{|D_{j,t}|-|Q_{j,t}|-1}, \tag{6.13}$$

pois $|D_{j,t}| - |Q_{j,t}| - 1$ é o menor número de erros capaz de gerar $Q_{j,t}$, uma vez que apenas um pacote em *outage* é o evento mais provável dado que ocorreu *outage*, como ilustrado na Figura 6.2. Como $j \in D_{j,t}$ e $j \notin Q_{j,t}$, a seguinte relação deve ser satisfeita:

$$\Delta_{j,t} \triangleq |D_{j,t}| - |Q_{j,t}| \geq 1. \tag{6.14}$$

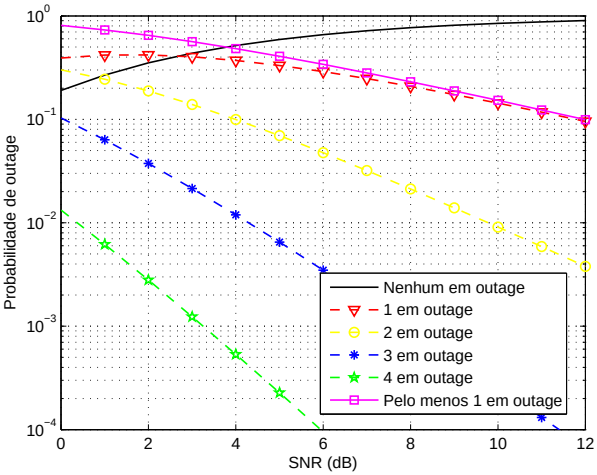


Figura 6.2: Probabilidade de *outage* versus SNR, para uma rede com $M = 2$ usuários e parâmetro $k_1 = 2$ e considerando todas as possíveis ocorrências de *outage*. Percebe-se que dado que houve *outage*, muito provavelmente somente um dentre os $Mk_1 = 4$ pacotes estará em outage.

De acordo com (6.8), os usuários pertencentes a $Q_{j,t}$ contribuirão com k_2' pacotes de verificação de paridade na fase de cooperação,

enquanto que os usuários pertencentes ao conjunto complementar $D_{j,t}\backslash Q_{j,t}$ contribuirão com k_2 pacotes de verificação de paridade. Assim sendo, a mensagem $I_j(t)$ está contida em $(|D_{j,t}|-|Q_{j,t}|)k_2+|Q_{j,t}|k_2'+1$ pacotes (1 da parte sistemática mais $(|D_{j,t}|-|Q_{j,t}|)k_2+|Q_{j,t}|k_2'$ como parte de paridades) transmitidos para a ERB por canais independentes. Para $D_{j,t}$ e $Q_{j,t}$ fixos, pode-se mostrar que a probabilidade da ERB não conseguir recuperar $I_j(t)$ é

$$P_{o,j}(D_{j,t},Q_{j,t}) \approx \gamma P_e^{(|D_{j,t}|-|Q_{j,t}|)k_2+|Q_{j,t}|k_2'+1},$$

em que γ é a abreviação de $\gamma(k_1,k_2,D_{j,t},Q_{j,t})$, um inteiro positivo representando o número (multiplicidade) dos padrões de *outage* que resultam na mesma probabilidade. A probabilidade de *outage* total é finalmente dada por

$$\begin{aligned}
P_{o,j} &\approx \sum_{D_{j,t}}\sum_{Q_{j,t}} P_{D_{j,t}} P_{Q_{j,t}} P_{o,j}(D_{j,t},Q_{j,t}) && \text{(6.15a)}\\
&\approx \sum_{D_{j,t}}\sum_{Q_{j,t}} \gamma P_e^{M+(|D_{j,t}|-|Q_{j,t}|)k_2+(k2'-1)|Q_{j,t}|} && \text{(6.15b)}\\
&\approx \gamma' P_e^{M+\Delta^* k_2+(k2'-1)|Q_{j,t}|} && \text{(6.15c)}\\
&= \gamma' P_e^{M+k_2+(k2'-1)|Q_{j,t}|}, && \text{(6.15d)}
\end{aligned}$$

em que $P_{D_{j,t}}$ e $P_{Q_{j,t}}$ são dadas por (6.12) e (6.13), respectivamente, Δ^* corresponde ao valor de $\Delta_{j,k}=|D_{j,t}|-|Q_{j,t}|$ que resulta no termo de menor expoente em (6.15b), o qual é $|\Delta|^*=1$ de acordo com (6.14), e γ' coleta as multiplicidades de todos os eventos $D_{j,t}$ e $Q_{j,t}$ para os quais $|D_{j,t}|-|Q_{j,t}|=\Delta^*$.

Com relação ao parâmetro k_2' em (6.15d), pode-se ver que o seu menor valor para que a mesma diversidade do esquema GDNC original seja atingida é $k_2'=1$. Quando $k_2'=0$, a ordem de diversidade é diminuída pelo fator $|Q_{j,t}|$. Por outro lado, quando $k_2'\geq 1$, a ordem de diversidade não é maior que $M+k_2$, pois $Q_{j,t}$ com $|Q_{j,t}|=0$ (*i.e.*, conjunto vazio) é um evento possível que resulta em $M+k_2$ como o menor expoente. Assim sendo, fica provado que a ordem de diversidade da Abordagem 2 continua sendo $M+k_2$ se o parâmetro k_2' for escolhido como 1.

Como a taxa do código é adaptativa e pode assumir diferentes valores, uma quantidade maior de códigos de rede distintos (com diferentes taxas) necessita estar disponível aos usuários. Porém, tais códigos podem ser obtidos de códigos como os apresentados nas

Tabelas 5.2 e 5.3 através da operação de puncionamento.

6.3 Simulações

Nesta seção, alguns resultados de simulações são apresentados com o intuito de atestar os resultados obtidos analiticamente. Através das simulações, a taxa de informação R foi considerada como sendo igual a 0.5 bits por uso do canal[2].

A Fig. 6.3 apresenta a taxa média em função da SNR para uma rede com 2 usuários com parâmetro $k_1 = 2$, considerando o esquema GDNC com $k_2 = 2$, a Abordagem 1 com $k_2 \in \{0, 2\}$ e a Abordagem 2 com $k_{2,j} \in \{0, 1 \text{ e } 2\}$. A taxa do esquema GDNC não varia com a SNR, e para os parâmetros dados é igual a 0.5 (o mesmo acontece para os esquemas BNC e DNC). Pode-se notar que, na Abordagem 1, apenas um bit de retorno para cada bloco de Mk_1 pacotes de informação é suficiente para aumentar suficientemente a taxa. Se a quantidade de retorno é aumentada para um bit por usuário, de acordo com a Abordagem 2, percebe-se que a taxa é aumentada ainda mais. Pode-se também notar que os resultados de simulação coincidem perfeitamente com os resultados analíticos.

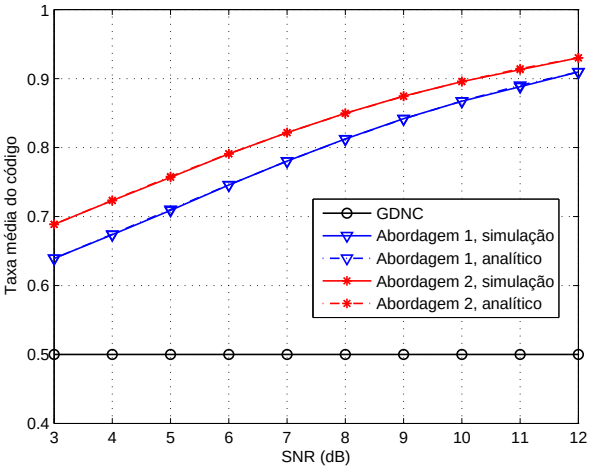


Figura 6.3: Taxa média versus SNR (dB) para uma rede com 2 usuários e $k_1 = 2$, considerando o esquema GDNC com $k_2 = 2$, a Abordagem 1 com $k_2 \in \{0, 2\}$ e a Abordagem 2 com $k_{2,j} \in \{0, 1, 2\}$.

[2]Recordando que a ordem de diversidade não depende da escolha da taxa de transmissão, como mostrado na Seção 4.1.2.

No que diz respeito à probabilidade de *outage* e à ordem de diversidade, a Fig. 6.4 apresenta a FER em função da SNR para a mesma rede com 2 usuários considerada na Fig. 6.3, considerando também os esquemas BNC e DNC (DNC sobre GF(4)). As matrizes geradoras utilizadas estão apresentadas na Tabela 5.2. Novamente, assume-se a existência de um código de canal capaz de recuperar o pacote transmitido sempre que $|h_{j,i,t}|^2 \geq g$. Se $|h_{j,i,t}|^2 < g$, uma *outage* é declarada. Como esperado, ambas as abordagens propostas

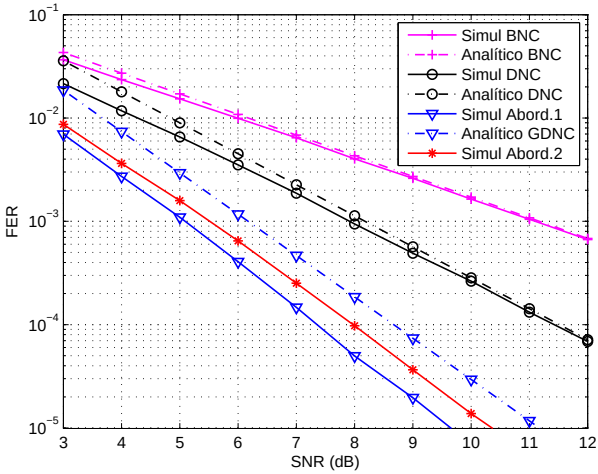


Figura 6.4: FER versus SNR (dB) para uma rede com 2 usuários, considerando os esquemas BNC, DNC (sobre GF(4)), Abordagem 1 com $k_1 = 2$ e $k_2 = \{0, 2\}$ e Abordagem 2 com $k_1 = 1$ e $k_{2,j} = \{0, 1, 2\}$, ambos sobre GF(8) e com código obtido da Tabela 5.2. Relembrando que o esquema GDNC (com $k_1 = k_2 = 2$ e sobre GF(8)) possui o mesmo desempenho que a Abordagem 1.

apresentam a mesma diversidade que o esquema GDNC, superando os esquemas BNC e DNC. Como o código na Abordagem 2 é composto por uma quantidade menor de paridade se comparado com a Abordagem 1, o desempenho inferior em termos de ganho de codificação já era esperado.

Quando o número de usuários aumenta, o comportamento assintótico das abordagens propostas é diferente. Isso está ilustrado na Figura 6.5, na qual a taxa média é plotada em função do número de usuários para uma rede com SNR média igual a 10 dB, considerando os esquemas GDNC com $k_2 = 2$, a Abordagem 1 com $k_2 = \{0, 2\}$ e a Abordagem 2 com $k_{2,j} = \{0, 1, 2\}$, todos com $k_1 = 2$. Pode-se ver

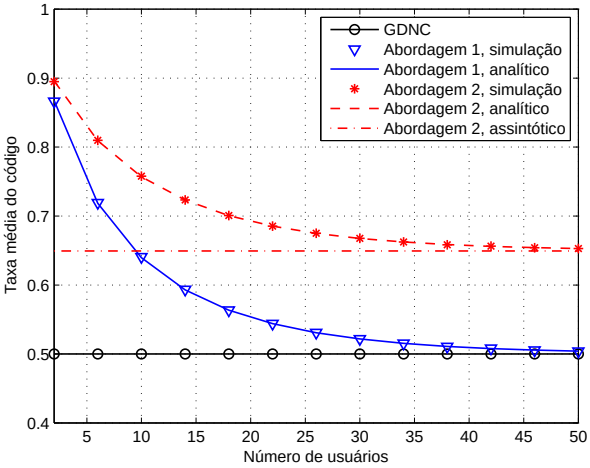


Figura 6.5: Taxa média em função do número de usuários M para uma rede com $k_1 = 2$ e SNR $= 10$ dB, considerando o esquema GDNC com $k_2 = 2$, a Abordagem 1 com $k_2 \in \{0, 2\}$ e a Abordagem 2 com $k_{2,j} \in \{0, 1, 2\}$.

que, enquanto a taxa da Abordagem 1 tende para a mesma taxa do esquema GDNC, a taxa da Abordagem 2 tende para um valor mais elevado, confirmando as expectativas.

6.4 Comentários

Neste capítulo, uma variante do esquema GDNC foi proposta, a qual visa evitar a transmissão de pacotes de verificação de paridade desnecessários através da consideração de existência de um canal de retorno entre a ERB e os usuários. Por este canal de retorno, considerado livre de erro, é transmitida uma pequena quantidade de informação relativa ao sucesso/fracasso na decodificação dos pacotes de informação recebidos durante a fase de difusão. De acordo com a informação recebida da ERB, os usuários projetam os códigos de rede de forma adaptativa, mantendo a mesma ordem de diversidade e maximizando a taxa de transmissão.

A consideração de canal de retorno livre de erros é uma consideração razoável, visto que a quantidade de informação transmitida é pequena e pode ser transmitida a uma taxa de transmissão baixa o suficiente para tornar a transmissão altamente confiável.

Capítulo 7

Comentários Finais

NESTE trabalho de doutorado, conceitos de códigos corretores de erros clássicos foram utilizados no projeto de códigos de rede com o intuito de melhorar o desempenho de erro de uma rede de múltiplo acesso em que os usuários são aptos a cooperar entre si. Percebeu-se que, na situação em que os canais interusuário são livres de erros, a habilidade do receptor para recuperar os pacotes de informação a partir dos pacotes recebidos corretamente é equivalente à capacidade de correção de apagamento do código do bloco associado à matriz de transferência da rede, de tal forma que a ordem de diversidade do sistema desempenha o mesmo papel que a distância mínima de Hamming do referido código de bloco.

Assim sendo, utilizando o limitante de Singleton como um limitante superior para a ordem de diversidade, foi proposto o esquema de *codificação de rede dinâmica e generalizada* (GDNC), uma generalização do esquema de codificação de rede dinâmica (DNC) proposto em [18]. Como os canais interusuário não são livres de erros na prática, a ordem de diversidade dada pelo limitante superior de Singleton não pode ser atingida. Mostrou-se através de uma análise de probabilidade de *outage* qual a ordem de diversidade atingida pelo esquema GDNC, a qual mostrou-se ser maior que a atingida pelo esquema DNC, se uma mesma taxa for considerada. Mais que isso, foi mostrado que com o esquema GDNC, além da ordem de diversidade, pode-se ao mesmo tempo atingir taxa de transmissão mais elevada que no esquema DNC.

Do ponto de vista do projeto de códigos capazes de atingir a ordem de diversidade no esquema GDNC, desenvolveu-se uma teoria, denominada "teoria das matrizes deficientes", para demonstrar que se a matriz

geradora de um código de bloco (na sua forma sistemática) MDS for utilizada como a matriz de transferência da rede, a máxima diversidade é garantida. Dessa forma, uma matriz geradora de qualquer código MDS pode ser utilizada como matriz de transferência no esquema GDNC, como por exemplo as da bem conhecida classe de códigos Reed-Solomon, não havendo a necessidade de projetar o código levando em conta todos os possíveis padrões de erro da rede, como no esquema DNC, o que pode se tornar muito complexo à medida que o número de usuários aumenta.

Uma variante do esquema GDNC foi também proposta, visando evitar a transmissão de pacotes de paridade desnecessários e consequentemente aumentar a taxa de transmissão do sistema como um todo. Para tal, foi assumida a existência de um canal de retorno entre a ERB e os usuários, através do qual uma pequena quantidade de informação relativa ao sucesso/fracasso na decodificação dos pacotes recebidos durante a fase de difusão é transmitida pela ERB. Em posse desta informação, os usuários são aptos a projetar o código de rede de forma adaptativa, reduzindo a quantidade de pacotes de paridade quando conveniente.

Para ambas as variantes do esquema GDNC propostas, com e sem canal de retorno, análises da probabilidade de *outage* foram desenvolvidas a fim de avaliar a ordem de diversidade atingida pelos esquemas propostos. Simulações computacionais foram realizadas e confirmaram os resultados obtidos de forma analítica, tanto em termos de ordem de diversidade quanto em termos de taxa de transmissão.

À medida que o número de usuários cresce, a complexidade de decodificação inerente ao esquema proposto (decodificação de códigos Reed Solomon) pode se tornar impraticável. Nesta situação, como trabalho futuro, pretende-se considerar como código de rede uma matriz geradora de um código de bloco de baixa densidade, ou seja, uma matriz geradora esparsa, em que os usuários, quando agindo como retransmissores, realizem uma combinação linear (sobre corpos finitos suficientemente grandes) de apenas um subconjunto das mensagens que decodificaram corretamente durante a fase de difusão. Do ponto de vista da ERB, o efeito de um código LDPC (ou LDGM) distribuído seria formado, a exemplo do esquema ANCC (do inglês *Adaptive Network Coded Cooperation*) proposto em [73].

Outra ideia de interesse prático seria considerar que os usuários não são capazes de informar à ERB como as combinações lineares são geradas, isto é, qual a situação instantânea dos canais interusuário. Nesse caso, a ERB teria que lidar com correção de apagamentos e de erros ao mesmo tempo. Certamente, a ordem de diversidade do sistema

seria reduzida.

Apêndice A

Campos Finitos (de Galois)

Este apêndice tem como objetivo introduzir o conceito de campos finitos (também chamados de campos de Galois), os quais possuem fundamental importância no projeto de códigos corretores de erros. Inicialmente, uma estrutura algébrica denominada grupo será apresentada, para em seguida serem apresentadas operações polinomiais sobre essas estruturas. A utilidade disso tudo no projeto de códigos corretores de erros reside no fato de que um polinômio definido sobre um campo finito GF(p) (em que p é um número primo), possui suas raízes naquele campo, ou em algum campo estendido GF(q). De forma similar, cada elemento a do campo finito estendido GF(q) é uma raiz de alguns polinômios com coeficientes pertencentes ao campo finito GF(p). O polinômio com grau mínimo que satisfaz essa condição é denominado *polinômio mínimo* de a [74].

A.1 Grupos

Um grupo G_r é definido como um conjunto de elementos que estão relacionados por operações específicas. Um conjunto de elementos G_r sobre o qual a operação binária $\oplus$ é definida é dito ser um grupo se as seguintes condições forem satisfeitas:

(i) A operação binária $\oplus$ for associativa;

(ii) O conjunto de elementos G_r contiver um elemento e tal que, para cada elemento do conjunto $a \in G_r$,

$$a \oplus e = e \oplus a = a$$

O elemento e é chamado de identidade para a operação binária

$\oplus$.

(*iii*) Para cada elemento do conjunto $a \in G_r$, existir um outro elemento do mesmo conjunto $a' \in G_r$, tal que

$$a \oplus a' = a' \oplus a = e$$

O elemento a' é chamado o inverso do elemento a.

Um grupo G_r é dito ser comutativo se, para cada par de elementos $a, b \in G_r$, for verdade que

$$a \oplus b = b \oplus a$$

Pode-se também mostrar que tanto o elemento inverso a' de um elemento a quanto o identidade e da operação binária definida sobre o grupo G_r são únicos [74].

A.2 Adição e Multiplicação Módulo-m

Para o conjunto de elementos $G_r = \{0, 1, \ldots, i, \ldots, j, \ldots, m-1\}$ que satisfaça as condições para ser um grupo, a operação de adição $\boxplus$ entre quaisquer dois elementos i e j é definida como

$$i \boxplus j = r \tag{A.1a}$$

$$r = (i + j) \pmod{m} \tag{A.1b}$$

isso é, a adição de quaisquer dois elementos i e j pertencentes ao grupo G_r é o resto da divisão da adição aritmética $(i+j)$ por m. Essa operação é chamada adição módulo-m.

A multiplicação módulo-p entre quaisquer dois elementos i e j é definida como

$$i \boxtimes j = r \tag{A.2a}$$

$$r = ij \pmod{p} \tag{A.2b}$$

em que p é um número primo.

A.3 Campos

Com base na definição de grupos apresentada anteriormente, um campo finito é aqui definido como um conjunto de elementos F para o qual adição, multiplicação, subtração e divisão (exceto divisão por zero, a qual não é definida) realizadas entre seus elementos resultam em outro elemento do mesmo conjunto. O conjunto F^* é definido como o conjunto F original porém sem o elemento 0. Para as operações de

adição e multiplicação, as seguintes operações definem um campo:

(*i*) F é um grupo comutativo com respeito à operação de adição. O elemento identidade para a operação de adição é o elemento "0".
(*ii*) F^* é um grupo comutativo para a operação de multiplicação. O elemento identidade para a multiplicação é o elemento "1".
(*iii*) Multiplicação é distributiva com respeito à adição:

$$a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c)$$

O número de elementos do campo é chamado de *ordem* daquele campo. Um campo com um número finito de q elementos é usualmente chamado de campo finito, ou campo de Galois, e representado por $\mathbb{F}_q$ ou GF(q). O inverso aditivo de um elemento $a \in F$ é denotado por $-a$, e o inverso multiplicativo do elemento $a \in F^*$ é denotado por a^{-1}. Assim sendo, as operações de subtração e divisão sobre campos finitos são definidas como

$$a \boxminus b = a \boxplus (-b) \tag{A.3a}$$

$$a \div b = a \boxtimes (b^{-1}) \tag{A.3b}$$

Para um dado número primo p, o conjunto de números inteiros $\{0, 1, 2, \ldots, p-1\}$ é um grupo comutativo com respeito à adição módulo-p. O conjunto de números inteiros $\{1, 2, \ldots, p-1\}$ é um grupo comutativo com respeito à multiplicação módulo-p. Esse é portanto um campo de ordem p, denominado GF(p). Uma extensão do campo primo GF(p) é chamado campo estendido GF(q) = GF(p^m), em que m é um número inteiro positivo. Esse campo estendido é também denominado campo de Galois. Casos particulares de interesse prático são os campos finitos na forma GF(2^m), com m sendo um número inteiro positivo.

Pode-se também mostrar que se a é um elemento não-nulo de GF(q), então $a^{q-1} = 1$. Também é verdade que se a for um elemento não nulo pertencente ao campo finito GF(q), e se n é a ordem (expoente) daquele elemento, então n divide $q - 1$.

Um elemento não-nulo de um campo finito GF(q) é dito ser um elemento primitivo daquele campo se a ordem daquele elemento for $q-1$. Todas as potências de um número primitivo $a \in$ GF(q) geram todos os elementos não-nulos do campo GF(q). Cada campo finito possui pelo menos um elemento primitivo.

A.4 Polinômios sobre Campos Binários

Os campos mais frequentemente utilizados são extensões do campo binário GF(2), e são chamados campos de Galois GF(2^m). Aritmética binária utiliza adição e multiplicação módulo-2. Um polinômio $f(X)$ definido sobre GF(2) possui a forma

$$f(X) = f_0 + f_1X + f_2X^2 + \ldots + f_nX^n$$

em que os coeficientes f_i são 0 ou 1. O maior expoente da variável X é chamado o *grau do polinômio*.

Definição 2 *Um elemento a do campo é um zero ou raiz do polinômio $f(X)$ se $f(a) = 0$. Nesse caso, $X - a$ é um fator do polinômio $f(X)$.*

Definição 3 *Um polinômio $p(X)$ definido sobre GF(2), de grau m, é dito ser irredutível (ou primo) se $p(X)$ não possui nenhum polinômio fator de grau maior que zero ou menor que m. Além disso, um polinômio irredutível $p_i(X)$ de grau m é um polinômio primitivo se o menor número inteiro n para o qual $p_i(X)$ é um fator de X^n+1 for $n = 2^m-1$.*

A.5 Propriedades de Campos de Galois Estendidos GF(2^m)

Polinômios definidos sobre GF(2) podem também possuir raízes pertencendo a um campo estendido GF(2^m). Isso está apresentado no seguinte teorema [74].

Teorema A.1 *Seja $f(X)$ um polinômio definido sobre GF(2). Se um elemento β do campo de Galois estendido GF(2^m) é uma raiz do polinômio $f(X)$, então para qualquer inteiro $l \geq 0, \beta^{2^l}$ é também raiz daquele polinômio.*

A.6 Polinômios Mínimos

Como cada elemento do campo de Galois GF(2^m) é uma raiz do polinômio $X^{2^m} + X$, o mesmo elemento poderia ser uma raiz de um polinômio definido sobre GF(2) cujo grau é menor que 2^m.

Definição 4 *O polinômio de grau mínimo $\phi(X)$, definido sobre GF(2) que possui β como sua raiz, é chamado o polinômio mínimo de β.*

Assim sendo, o polinômio mínimo do elemento 0 é X, e o polinômio mínimo do elemento 1 é $1 + X$.

A.6.1 Propriedades de Polinômios Mínimos

Algumas propriedades de polinômios mínimos são listadas a seguir [44]:

(*i*) O polinômio mínimo de um elemento β de um campo de Galois GF(2^m) é um polinômio irredutível.

(*ii*) Para um dado polinômio $f(X)$ definido sobre GF(2), and $\phi(X)$ sendo o polinômio mínimo de β, se β for uma raiz de $f(X)$, consequentemente $\phi(X)$ é um fator de $f(X)$.

(*iii*) O polinômio mínimo $\phi(X)$ do elemento β do campo de Galois GF(2^m) é um fator de $X^{2^m} + X$.

(*iv*) Seja $f(X)$ um polinômio irredutível definido sobre GF(2), e $\phi(X)$ o polinômio mínimo de um elemento β de um campo de Galois GF(2^m). Se $f(\beta) = 0$, então $f(X) = \phi(X)$.

(*v*) Seja $\phi(X)$ o polinômio mínimo do elemento β do campo de Galois GF(2^m), e seja e o menor número inteiro para o qual $\beta^{2^e} = \beta$, então o polinômio mínimo de β será

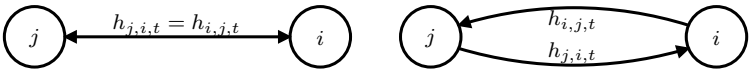
$$\phi(X) = \Pi_{i=0}^{e-1}(X + \beta^{2^i})$$

Para mais detalhes a respeito de campos finitos, sugerem-se as referências [51], [44],[36].

Apêndice B

Cálculo da Probabilidade de *Outage*

Inicialmente, considere a Figura B.1, a qual ilustra o conceito de reciprocidade.



(a) Canais recíprocos. (b) Canais não-recíprocos.

Figura B.1: Ilustração de canais recíprocos e não-recíprocos. O índice t indica o *slot* de tempo.

Nos exemplos inicias dos esquemas DNC e GDNC ilustrados respectivamente pelas Figuras 4.4 e 5.1, o cálculo da probabilidade de *outage* foi desenvolvido baseado na suposição de canais interusuário recíprocos, de acordo com o apresentado na Figura B.1(a).

Este apêndice tem por objetivo recalcular a probabilidade de *outage* de tais exemplos considerando a situação em que os canais interusuário não são recíprocos. O procedimento para o cálculo é o mesmo, a diferença reside na quantidade de combinações que deve ser analisada, a qual torna-se maior.

Seja uma rede com M usuários. Existem $M-1$ canais recíprocos entre cada usuário e seus parceiros, resultando em 2^{M-1} possibilidades distintas de *outage* para estes canais. Para o caso em que os canais são não-recíprocos, existem $2(M-1)$ canais (não importa em qual

sentido) entre cada usuário e seus parceiros, resultando em $2^{2(M-1)}$ possibilidades.

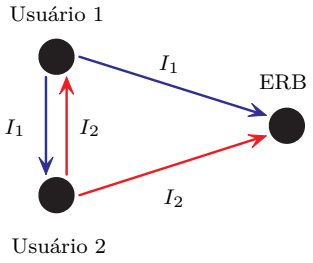


Figura B.2: Fase de difusão para rede com $M = 2$ usuários.

Assim sendo, como os exemplos introdutórios do esquema DNC e GDNC consideram $M = 2$ usuários, de acordo com a Figura B.2, temos 2 combinações diferentes para o caso em que os canais são recíprocos (estar em *outage* ou não estar em *outage*). Já para canais não-recíprocos, a quantidade a ser avaliada é igual a $2^{2(M-1)} = 4$. Tais possibilidades estão apresentadas na Tabela B.1, calculadas de acordo com a Seção 4.1.1.

Tabela B.1: Possibilidades de *outage* para canais interusuário e $M = 2$ usuários. OUT= 1/0 significa que o enlace está/não está em *outage*.

Situação S	link $1 \rightarrow 2$	link $2 \rightarrow 1$	$\Pr\{S\}$
S_1	OUT $= 0$	OUT $= 0$	$(1-P_e)^2$
S_2	OUT $= 0$	OUT $= 1$	$(1-P_e)P_e$
S_3	OUT $= 1$	OUT $= 0$	$P_e(1-P_e)$
S_4	OUT $= 1$	OUT $= 1$	P_e^2

No que se segue tais probabilidades serão recalculadas levando em consideração todas estas possibilidades de *outage* para os canais interusuário.

B.1 DNC com canais não recíprocos para M=2 usuários

Focando no Usuário 1 (o mesmo resultado vale para o Usuário 2 devido à simetria do sistema), tem-se as seguintes condições de *outage*

para a mensagem I_1 de acordo com as situações dos canais interusuário apresentadas na Tabela B.1:

Situação S_1: Os pacotes I_1, I_2, $I_1 \oplus I_2$ e $I_1 \oplus 2I_2$ são transmitidos para a ERB. Uma *outage* ocorre quando a transmissão direta do pacote I_1 *e* pelo menos 2 dos 3 pacotes restantes não são decodificados corretamente. Isso ocorre com probabilidade [18]

$$P_1 = P_e \left[\binom{3}{2} P_e^2 (1 - P_e) + P_e^3 \right] \approx 3P_e^3.$$

Situação S_2: Os pacotes I_1, I_2, I_1 e $I_1 \oplus 2I_2$ são transmitidos para a ERB. Ao receber dois pacotes, a ERB realiza MRC. Uma *outage* ocorre quando a transmissão direta do pacote I_1 *e* pelo menos 1 dos 2 pacotes restantes não são decodificados corretamente. Isso ocorre com probabilidade

$$P_2 = \frac{P_e^2}{2} \left[2P_e(1 - P_e) + P_e^2 \right] \approx P_e^3.$$

Situação S_3: Os pacotes I_1, I_2, $I_1 \oplus I_2$ e I_2 são transmitidos para a ERB. Uma *outage* ocorre quando a transmissão direta do pacote I_1 *e* pelo menos 1 dos 2 pacotes restantes não são decodificados corretamente. Isso ocorre com probabilidade [18]

$$P_3 = P_e \left[\frac{P_e^2}{2}(1 - P_e) + P_e(1 - \frac{P_e^2}{2}) + \frac{P_e^3}{2} \right] \approx P_e^2.$$

Situação S_4: Os pacotes I_1, I_2, I_1 e I_2 são transmitidos para a ERB. Ao realizar MRC a probabilidade de *outage* para I_1 é

$$P_4 = \frac{P_e^2}{2}.$$

A probabilidade de *outage* total é então dada por:

$$P_{\text{o,DNC}} \approx \sum_{i=1}^{4} P_i \Pr\{S_i\} \approx 4P_e^3. \tag{B.1}$$

B.2 GDNC com canais não recíprocos para M=2 usuários e taxa 6/10

Para o esquema GDNC, será analisada a probabilidade de *outage* da mensagem do Usuário 1 no *slot* de tempo 1, denotada $I_1(1)$. Novamente,

a exemplo da Seção 5.1, a multiplicidade dos padrões de erro que resultam na mesma probabilidade de *outage* não será considerada, pois é difícil (se possível) de ser obtida através deste tipo de análise. A atenção aqui concentra-se no expoente da probabilidade de *outage*. As situações a seguir referem-se à Tabela B.1.

(*i*) Situação S_1: 5 pacotes contendo $I_1(1)$ são transmitidos para a ERB, com probabilidade de *outage* da ordem de

$$P_1 \approx P_e^5.$$

(*ii*) Situação S_2: 5 pacotes contendo $I_1(1)$ são transmitidos para a ERB, com probabilidade de *outage* da ordem de

$$P_2 \approx P_e^5.$$

(*iii*) Situação S_3: 3 pacotes contendo $I_1(1)$ são transmitidos para a ERB, com probabilidade de *outage* da ordem de

$$P_3 \approx P_e^3.$$

(*iv*) Situação S_4: 3 pacotes contendo $I_1(1)$ são transmitidos para a ERB, com probabilidade de *outage* da ordem de

$$P_4 \approx P_e^3.$$

Probabilidade de *outage* total:

$$P_{\text{o,GDNC}} \approx \sum_{i=1}^{4} P_i \Pr\{S_i\} \approx P_e^4. \tag{B.2}$$

Referências Bibliográficas

[1] Anatel, "Números do setor," September 2010. [Online]. Available: www.anatel.gov.br

[2] B. Emerson, "M2M: the internet of 50 billion devices," *Win-Win (Huawei)*, 2010. [Online]. Available: http://www.huawei.com/publications

[3] C. Shannon, "A mathematical theory of communications," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423 e 623–656, 1948.

[4] R. G. Gallager, "Low density parity check codes," *Transactions of the IRE Professional Group Inf. Theory*, vol. IT-8, pp. 21–28, January 1962.

[5] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Transactions on Information Theory*, vol. IT-13, pp. 260–269, April 1967.

[6] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near-Shannon limit error-correting coding and decoding: Turbo codes," in *Proc. IEEE Int. Conf. Commun.*, vol. 2, May 1993, pp. 1064–1070.

[7] M. C. Davey and D. J. MacKay, "Low-density parity check codes over GF(q)," *IEEE Communications Letters*, vol. 2, no. 6, pp. 165–167, June 1998.

[8] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, March 1999.

[9] S. X. Ng, O. R. Alamri, Y. Li, J. Kliewer, and L. Hanzo, "Near-capacity turbo trellis coded modulation design based on EXIT charts and union bounds," *IEEE Transactions on Communications*, vol. 56, no. 12, pp. 2030–2039, December 2008.

[10] G. J. Byers and F. Takawira, "Fourier transform decoding of non-binary LDPC codes," in *Proc. Southern African Telecommun. Networks and Applications Conf., SATNAC'04*, South Africa, September 2004.

[11] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 2809 – 2825, November 2003.

[12] R. Koetter, "On algebraic decoding of algebraic-geometric and cyclic codes," Ph.D. dissertation, Univ. Linköping, Linköping, 1996.

[13] C. Spagnol, "Aspects of LDPC codes for hardware implementation," Ph.D. dissertation, National University of Ireland, Cork, 2009.

[14] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity: Part I and Part II," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1948, November 2003.

[15] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage bahavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, December 2004.

[16] T. E. Hunter and A. Nosratinia, "Cooperative diversity through coding," in *Proc. IEEE Int. Symp. Inf. Theory, ISIT'02*, Lausanne, Switzerland, July 2002, p. 220.

[17] L. Xiao, T. Fuja, J. Kliewer, and D. Costello, "A network coding approach to cooperative diversity," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3714–3722, October 2007.

[18] M. Xiao and M. Skoglund, "M-user cooperative wireless communications based on nonbinary network codes," in *Proc. IEEE Inf. Theory Workshop. ITW'09*, June 2009, pp. 316 – 320.

[19] ——, "Design of network codes for multiple-user multiple-relay wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory. ISIT'09*, June 2009, pp. 2562 – 2566.

[20] J. L. Rebelatto, B. F. Uchôa-Filho, Y. Li, and B. Vucetic, "Generalized distributed network coding based on nonbinary linear block codes for multi-user cooperative communications," in *Proc. IEEE Int. Symp. Inf. Theory, ISIT'10*, June 2010, pp. 943–947.

[21] ——, "Multi-user cooperative diversity through network coding based on classical coding theory," *Submitted to IEEE Trans. Inf. Theory*, 2010. [Online]. Available: http://arxiv.org/abs/1004.2757

[22] G. M. Geronymo, J. L. Rebelatto, and B. F. Uchôa-Filho, "Feedback-assisted adaptive network coded cooperation for wireless networks," in *Proc. of the 2010 International Telecommun. Symp. (ITS'10)*, Manaus, Brazil, 2010.

[23] J. L. Rebelatto, B. F. Uchôa-Filho, Y. Li, and B. Vucetic, "Adaptive distributed network-channel coding for cooperative multiple access channel," in *To appear in the Proc. IEEE International Conf. on Commun. (ICC'11)*, Kyoto, Japan, 2011.

[24] C. Hausl and P. Dupraz, "Joint network-channel coding for the multiple-access relay channel," in *Proc. 3rd Annual IEEE Commun. Soc. Sensor and Ad Hoc Commun. and Netw. SECON '06*, vol. 3, September 2006, pp. 817 –822.

[25] C. Hausl, "Joint network-channel coding for wireless relay networks," Ph.D. dissertation, Technischen Universität München, Munich, 2008.

[26] D. Bing and Z. Jun, "Design and optimization of joint network-channel LDPC code for wireless cooperative communications," in *Proc. Int. Conf. Commun. Systems. ICCS'08*, November 2008, pp. 1625 –1629.

[27] M. Dohler and Y. Li, *Cooperative Communications: Hardware, Channel & Phy*. Wiley, 2010.

[28] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204 – 1216, 2000.

[29] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Foundations and Trends® in Networking, Now Publishers Inc., 2007.

[30] ——, *Network Coding Applications*. Foundations and Trends® in Networking, Now Publishers Inc., 2007.

[31] N. Cai and R. Yeung, "Network coding and error correction," in *Proc. IEEE Inf. Theory Workshop (ITW'02)*, Bangalore, India, 2002, pp. 112–119.

[32] R. Yeung, S.-Y. Li, N. Cai, and Z. Zhang, *Network Coding Theory*. Foundation and Trends in Communications and Information Theory, 2005, vol. 2, no. 4 and 5.

[33] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. in Inf. and Systems*, vol. 6, no. 1, pp. 19–36, 2006.

[34] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. in Inf. and Systems*, vol. 6, no. 1, pp. 37–54, 2006.

[35] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 209 –218, January 2008.

[36] F. Macwilliams and N. Sloane, *The Theory of Error Correcting Codes*. Amsterdan: North Holland, 1977.

[37] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *SIAM Journal of Applied Mathematics*, vol. 8, pp. 300–304, 1960.

[38] "Google scholar," September 2010.

[39] H. V. Nguyen, S. X. Ng, L. Hanzo, J. L. Rebelatto, and Y. Li, "Near channel capacity network coding for multi-user cooperative communications," in *Submitted to IEEE Wireless Commun. & Netw. Conf. (WCNC'11)*, Cancun, Mexico, 2011.

[40] J. L. Rebelatto, B. F. Uchôa-Filho, and I. Baran, "Formatação de feixe oportunística para sistemas OFDMA sujeitos a desvanecimento lento," in *Proc. of the XXVI Simpósio Brasileiro de Telecomunicações (SBrT'08)*, Rio de Janeiro, Brazil, September 2008.

[41] J. L. Rebelatto and B. F. Uchôa-Filho, "Modelo de canal 3-hop com realimentação para sistemas de altas taxas," in *Proc. of the XXVII*

Simpósio Brasileiro de Telecomunicações (SBrT'09), Blumenau, Brazil, September 2009.

[42] J. L. Rebelatto, B. F. Uchôa-Filho, Y. Li, and B. Vucetic, "Adaptive distributed network-channel coding," *Submitted to IEEE Trans. Wirel. Commun.*, 2010.

[43] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782– 795, October 2003.

[44] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2004.

[45] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, pp. 147–160, 1950.

[46] R. H. Morelos-Zaragoza, *The Art Of Error Correcting Coding*. John Wiley & Sons, 2002.

[47] B. Vucetic and J. Yuan, *Turbo Codes: Principles and Applications*. Kluwer Academic Publishers, 2000.

[48] S. Lin and D. J. Costello Jr., *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

[49] C. B. Schlegel and L. C. Pérez, *Trellis and Turbo Coding*. John Wiley & Sons, 2004.

[50] T. K. Moon, *Error Correcting Codes - Mathematical Methods and Algorithms*. John Wiley & Sons, 2005.

[51] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Massachusetts: Kluwer, 1987.

[52] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres, Paris*, pp. 147–156, 1959.

[53] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inf. and Control 3*, pp. 68–79, 1960.

[54] ——, "Further results on error correcting binary group codes," *Inf. and Control 3*, pp. 279–290, 1960.

[55] D. C. Gorenstein and N. Zierler, "A class of error-correcting codes in pm symbols," *J. SIAM*, vol. 9, pp. 207–214, 1961.

[56] K. A. Bush, "Orthogonal arrays of index unity," in *Ann. Math. Stat.*, 1952, pp. 426–434.

[57] S. B. Wicker and V. K. Bhargava, *Reed-Solomon Codes and Their Applications*. IEEE Press, 1994.

[58] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*. Cambridge, 2003.

[59] R. W. da Nóbrega, "Códigos de subespaço aplicados a codificação de rede," Master's thesis, Universidade Federal de Santa Catarina, August 2009.

[60] D. B. West, *Introduction to Graph Theory*, 2nd ed. Prentice Hall, 2000.

[61] P. Elias, "Coding for noise channels," *IRE Conv. Rec.*, vol. 3, pp. 37–46, 1955.

[62] L. R. Ford and D. R. Fulkerson, "Maximal flow through a network," *Canadian Journal of Mathematics*, vol. 8, pp. 399–404, 1956.

[63] A. Zhan and C. He, "Joint design of channel coding and physical network coding for wireless networks," in *Proc. Int. Conf. Neural Netw. and Signal Processing*, June 2008, pp. 512 –516.

[64] Z. Zhang, "Network error correction coding in packetized networks," in *Proc. IEEE Inf. Theory Workshop (ITW'06b)*, Chengdu, China, October 2006, pp. 433–437.

[65] S. Jaggi, P. A. Chou, and K. Jain, "Low complexity algebraic network multicast codes," in *Proc. IEEE Int. Symp. on Inf. Theory, ISIT'03*, Yokohama, Japan, 2003.

[66] P. Sanders, S. Egner, and L. Tolhuizen, "Polynomial time algorithms for network information flow," in *Proc. 15th ACM Symposium on Parallel Algorithms and Architectures*, 2003.

[67] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge: Cambridge University Press, 2005.

[68] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, *MIMO Wireless Communications*. Cambridge University Press, 2007.

[69] M. Xiao and M. Skoglund, "Multiple-user cooperative communications based on linear network coding," *IEEE Transactions on Communications*, vol. 58, no. 12, pp. 3345–3351, December 2010.

[70] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, Accessed on 2010-01-02.

[71] SAGE, "Open source mathematics software," Online available at http://www.sagemath.org/.

[72] S. H. Friedberg, A. J. Insel, and L. E. Spence, *Linear Algebra*, 2nd ed. New Jersey: Pratince Hall, Engewood Cliffs, 1989.

[73] X. Bao and J. Li, "Adaptive network coded cooperation (ANCC) for wireless relay networks: Matching code-on-graph with network-on-graph," *IEEE Transactions on Wireless Communications*, vol. 7, no. 2, pp. 574–583, February 2008.

[74] J. C. Moreira and P. G. Farell, *Essentials of Error-Control Coding*. John Wiley & Sons, 2006.

Índice Remissivo

This page intentionally left blank.